



PRODUKTKATALOG 2015



Inhaltsverzeichnis

Das ist Fortinet

■ Überblick	3
■ Herausforderung – Sicherheit: der Kampf gegen moderne Bedrohungen	4
■ Herausforderung – Leistung: Sicherheit wird zum „Bremsklotz“	4
■ Herausforderung – Komplexität: Sicherheit ist zu komplex geworden	4
■ Sicherheit: FortiGuard Labs bietet schnelleren und effektiveren Schutz	4
■ Leistung: FortiASICs steigern die Leistung deutlich	5
■ Einfachheit: FortiOS ermöglicht Konsolidierung und Vereinfachung der Sicherheit	5
■ Hochleistungs-Lösungen	5
■ Mittlere Lösungen	6
■ Einstiegslösungen	6
■ Einsatzgebiete von Fortinet-Lösungen	
■ FortiGate – High Performance Next Generation Firewalling	8
■ FortiOS – Das Sicherheits-Betriebssystem der FortiGate-Serie	9

Die Module im einzelnen:

■ FortiGate Firewall	10
■ FortiGate VPN	10
■ FortiGate Intrusion Prevention Systeme (IPS)	11
■ FortiGate (D)DoS Abwehr	12
■ FortiGate Applikationskontrolle	12
■ FortiGate AntiVirus	14
■ FortiGate Web-Filter	15
■ FortiGate Secure WLAN	15
■ FortiGate Mobile Security und BYOD (Bring Your Own Device)	17
■ FortiGate Client Reputation	17
■ FortiGate Virtuelle Instanzen	18
■ FortiGate 2-Faktor-Authentifizierung mit FortiToken	19
■ FortiGate Data Loss Prevention	20
■ FortiGate WAN-Optimierung	20
■ FortiGate AntiSpam	21
■ FortiGate SSL-Inspection	21
■ FortiGate Bandbreiten-Management	21
■ FortiGate Layer 2 und Layer 3 Routing	21
■ FortiGate Netzwerkzugriffskontrolle (NAC)	22
■ FortiGate VoIP und SIP Security	22

■ FortiGate IPv6 Security	23
---------------------------	----

Eigenschaften auf einen Blick 25–26

■ FortiManager	27
■ FortiAnalyzer	28
■ FortiCloud	29
■ FortiAP – Sichere WLAN Infrastruktur mit den Access Points FortiAP	30
■ FortiPresence	32
■ FortiExtender 3G/4G WAN Extender	33
■ FortiConverter	33
■ FortiToken	34
■ FortiAuthenticator – Zentraler AAA-Server	36
■ FortiClient Endpoint Security	37
■ FortiSandbox	38
■ FortiMail	40
■ FortiWeb Web Application Firewall	41
■ FortiDB Datenbank-Sicherheit	42
■ FortiDDoS Abwehr von DDoS-Angriffen bis auf Applikationsebene	43
■ FortiDNS Schutz von DNS-Servern	44
■ FortiADC Application Level Load Balancing	45
■ Fortinet AscenLink WAN Link Load Balancing	45
■ FortiCache Bandbreite – eine ständige Herausforderung	46
■ FortinetVM Fortinet-Lösungen auch für VM-Systeme	47
■ FortiSwitch Gigabit Ethernet Switches	48
■ Network Access Control	48
■ PoE-Support	48
■ FortiCam und FortiRecorder IP-basierte Gebäudeüberwachung	48
■ Appliance oder VM ohne Lizenzgebühren	49
■ FortiBridge Hardware-FailOver-System	49
■ PoE Power-Injector	49
■ Rackmount Kits	49
■ FortiCare™	50
■ FortiGuard™ Gefahrenforschung und Umgang	50

Fortinet Produktmatrix 51–58

FORTINET®

Fortinet wurde im Jahr 2000 von Ken Xie, dem Gründer und ehemaligen Präsidenten und CEO von NetScreen gegründet. Ein starkes Management-Team mit großer Erfahrung in Sachen Netzwerksicherheit führt heute das Unternehmen.

Gründungsjahr: 2000

Erste Produktveröffentlichung:
Mai 2002

Börsengang: November 2009

NASDAQ: FTNT

Unternehmenszentrale

Sunnyvale, California

Mitarbeiter: mehr als 2.500

Umsatz 2013: 615 Mio. US-Dollar

Umsatz Quartal 2/2014:
184 Mio. US-Dollar

Anzahl verkaufte Produkte:
mehr als 1,6 Millionen

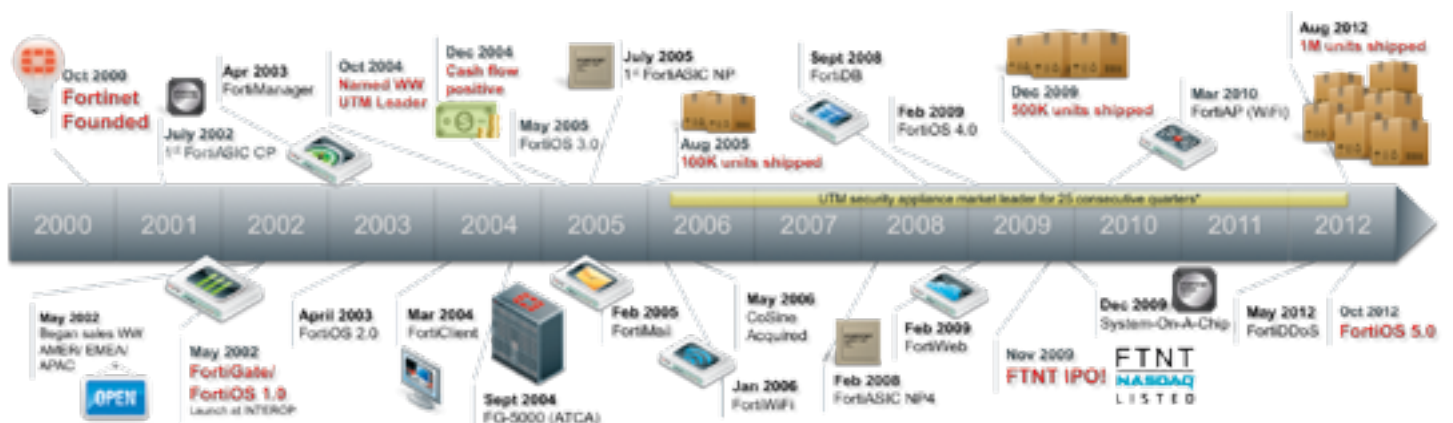
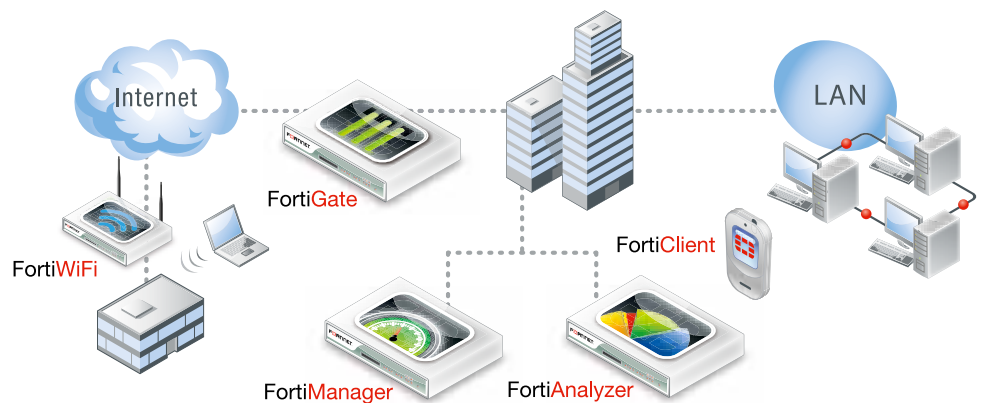
Kunden:
mehr als 200.000

Patente:
163 erteilte Patente
133 angemeldete Patente

■ Überblick

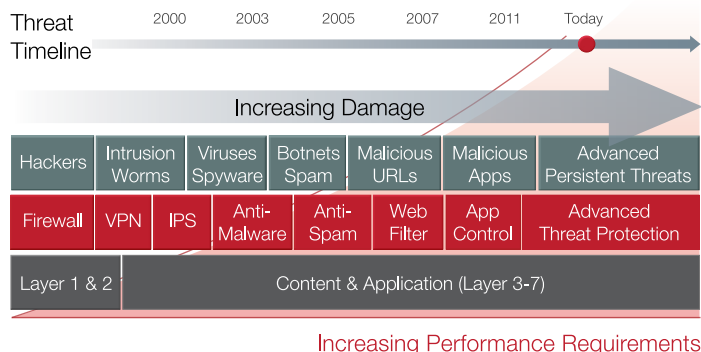
Die Mission von Fortinet ist es, innovativste und leistungsstärkste Netzwerk-Sicherheitsplattformen zu bieten und Ihre IT-Infrastruktur zu vereinfachen.

- Wir sind ein führender globaler Anbieter von Netzwerk-Sicherheitslösungen für Betreiber, Datenzentren, Unternehmen und verteilte Niederlassungen.
- Durch ständige Innovation unserer speziell angepassten ASICs, Hardwaresysteme, Netzwerksoftware, Verwaltungsmöglichkeiten und Sicherheitsforschung haben wir einen großen, schnell wachsenden und hochzufriedenen Kundenstamm und konnten Umsätze und Marktanteil ständig erhöhen.



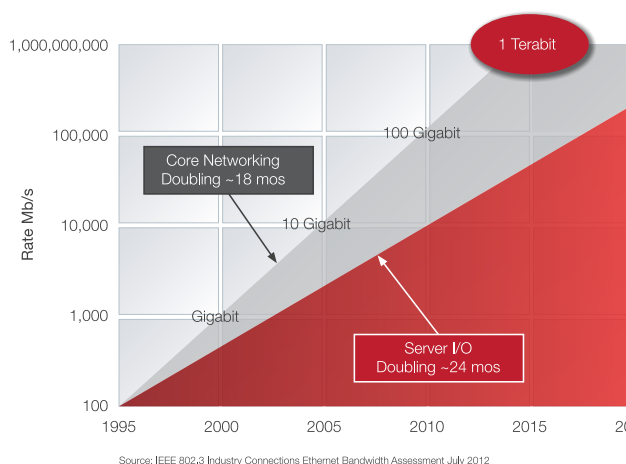
■ Herausforderung – Sicherheit: der Kampf gegen moderne Bedrohungen

- Die hoch entwickelten Bedrohungen unserer Zeit verursachen mehr Schaden als je zuvor.
- Die meisten Anbieter verlagern wichtige Aspekte der Bekämpfung nach außen oder bieten sie überhaupt nicht an.
- Unternehmen müssen Lösungen Stück für Stück entwickeln.



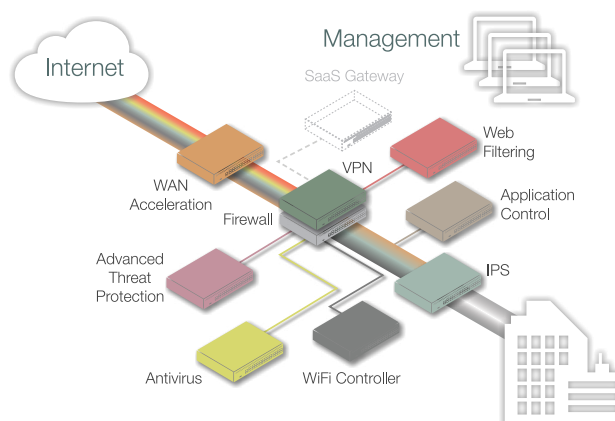
■ Herausforderung – Leistung: Sicherheit wird zum „Bremsklotz“

- Die Netzwerkbandweite muss wegen der wachsenden Anzahl an angeschlossenen Geräten, Datenvolumen, Virtualisierung, Cloud-Speicherung und SaaS-Anwendungen alle 18 Monate verdoppelt werden.
- Netzwerk-Sicherheitslösungen, die nicht schnell genug weiterentwickelt werden, werden zum Schwachpunkt und bremsen den wichtigen Traffic.



■ Herausforderung – Komplexität: Sicherheit ist zu komplex geworden

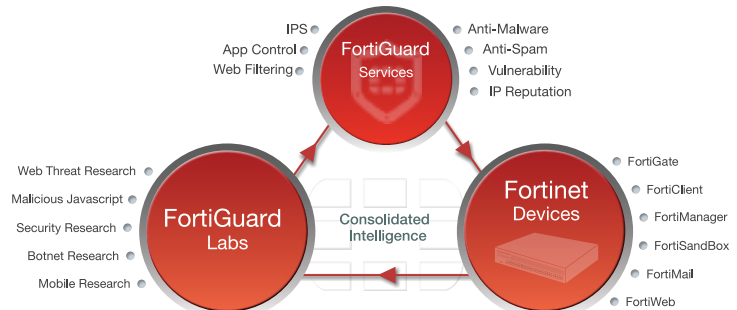
- Im Laufe der Zeit haben Unternehmen viele verschiedene punktuelle Lösungen gegen immer neue Bedrohungen eingesetzt.
- Zentrale, Filiale, Datenzentrum und Cloud nutzen unterschiedliche Plattformen.
- Viele Verwaltungskonsolen, uneinheitliche Regelungen und Funktionen sowie verschiedene Update-Zyklen führen zu langsamer und unzuverlässiger Reaktion auf neue Bedrohungen.



■ Sicherheit:

FortiGuard Labs bietet schnelleren und effektiveren Schutz

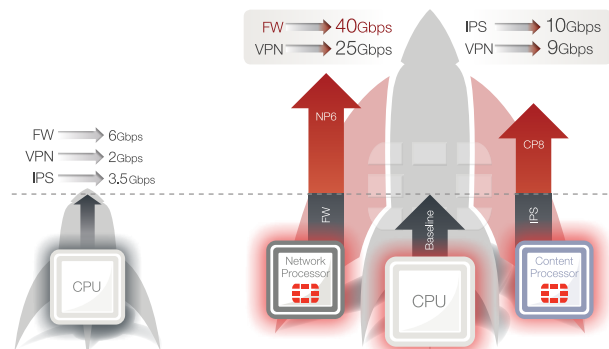
- Unser großes Forschungsteam für globale Bedrohungen erkennt neue Gefahren und entwickelt Schutzangebote für eine Vielzahl interner konsolidierter Sicherheitslösungen.
- Updates werden rund um die Uhr sofort geliefert.
- Der Schutz von FortiGuard wurde in unabhängigen Tests für hocheffektiv gegen aktuelle Bedrohungen befunden.



■ Leistung:

FortiASICs steigern die Leistung deutlich

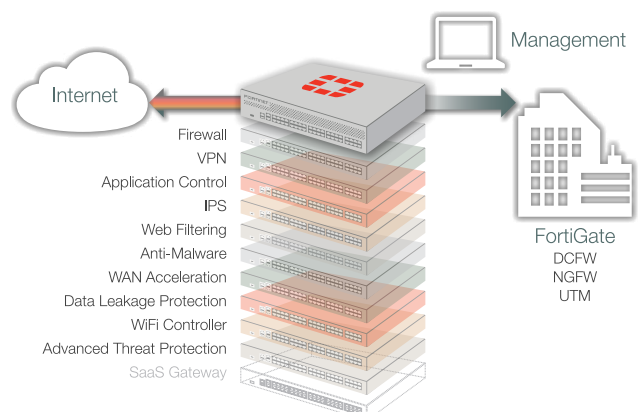
- Wichtige Netzwerk- und Contentverarbeitungsfunktionen werden von der CPU auf maßgeschneiderte FortiASICs geladen, um Leistung und Skalierbarkeit deutlich zu erhöhen.
- Unsere spezielle ASIC-Architektur bietet die beste Performance bei Netzwerksicherheitslösungen auf dem Markt, verhindert Engpässe und ermöglicht Kunden, den wachsenden Bandbreitenanforderungen nachzukommen.



■ Einfachheit:

FortiOS ermöglicht Konsolidierung und Vereinfachung der Sicherheit

- IT-Manager können einheitliche Grundsätze für alle Sicherheitslösungen schaffen und so schnellere, robustere Systeme mit weniger Verwaltungsaufwand entwickeln.
- Unsere integrierte Plattform bietet die Flexibilität, um Ressourcen dorthin zu verlagern, wo Sie sie brauchen. Sie erhalten eine einfachere und wartungsärmere Infrastruktur.



■ Hochleistungs-Lösungen

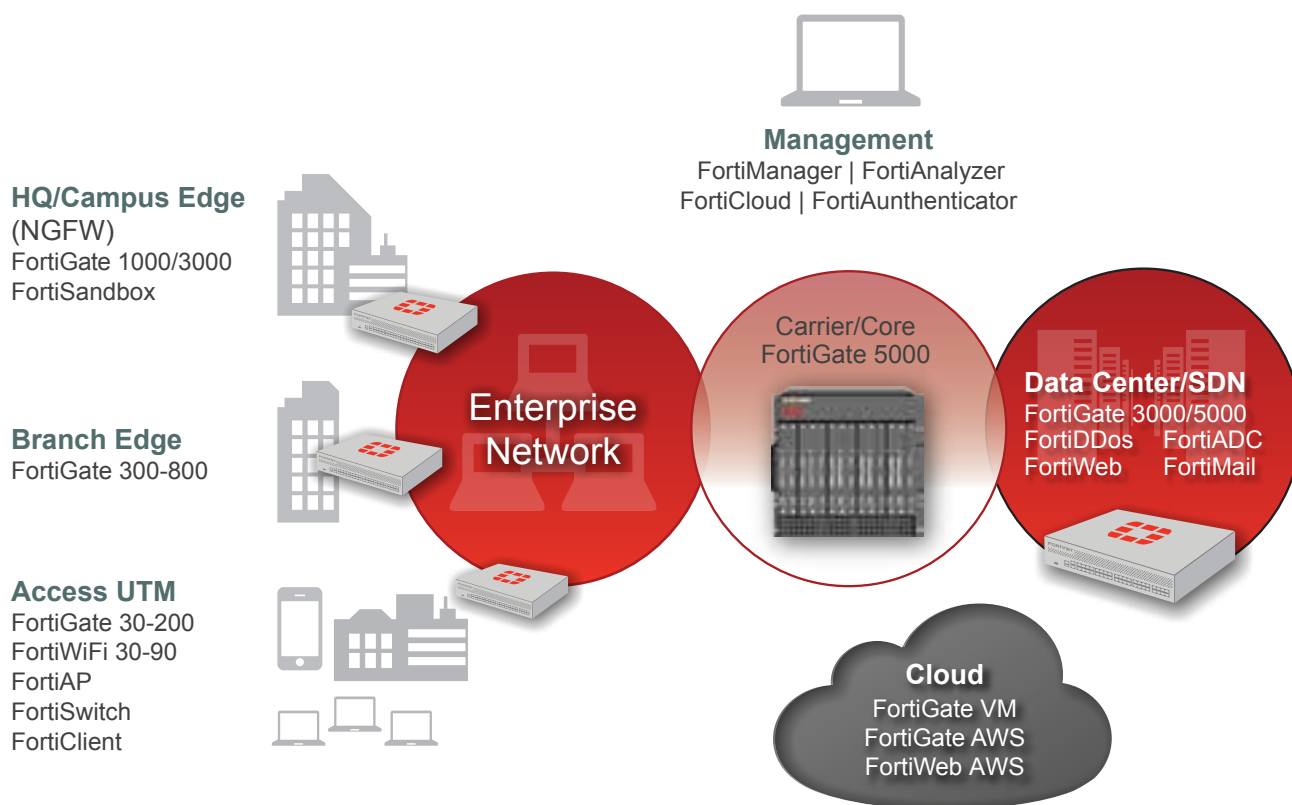
Die branchenführenden Hochleistungs-Sicherheitsplattformen von Fortinet bieten eine Next Generation Firewall (NGFW) mit außerordentlichem Datendurchlauf, äußerst niedriger Latenz und Multi-Vektor-Schutz, die sie zur idealen Lösung für anspruchsvollste Netzwerkumgebungen in Unternehmen macht.

■ Mittlere Lösungen

Mit unserem Sortiment an bewährten Hochleistungs-Sicherheitsplattformen finden Sie die richtige Balance zwischen Leistung und Preis für Ihre Anforderungen. Fortinet bietet mehr Modelle und Sicherheitstechnologie-Optionen als jeder andere Anbieter auf dem Markt.

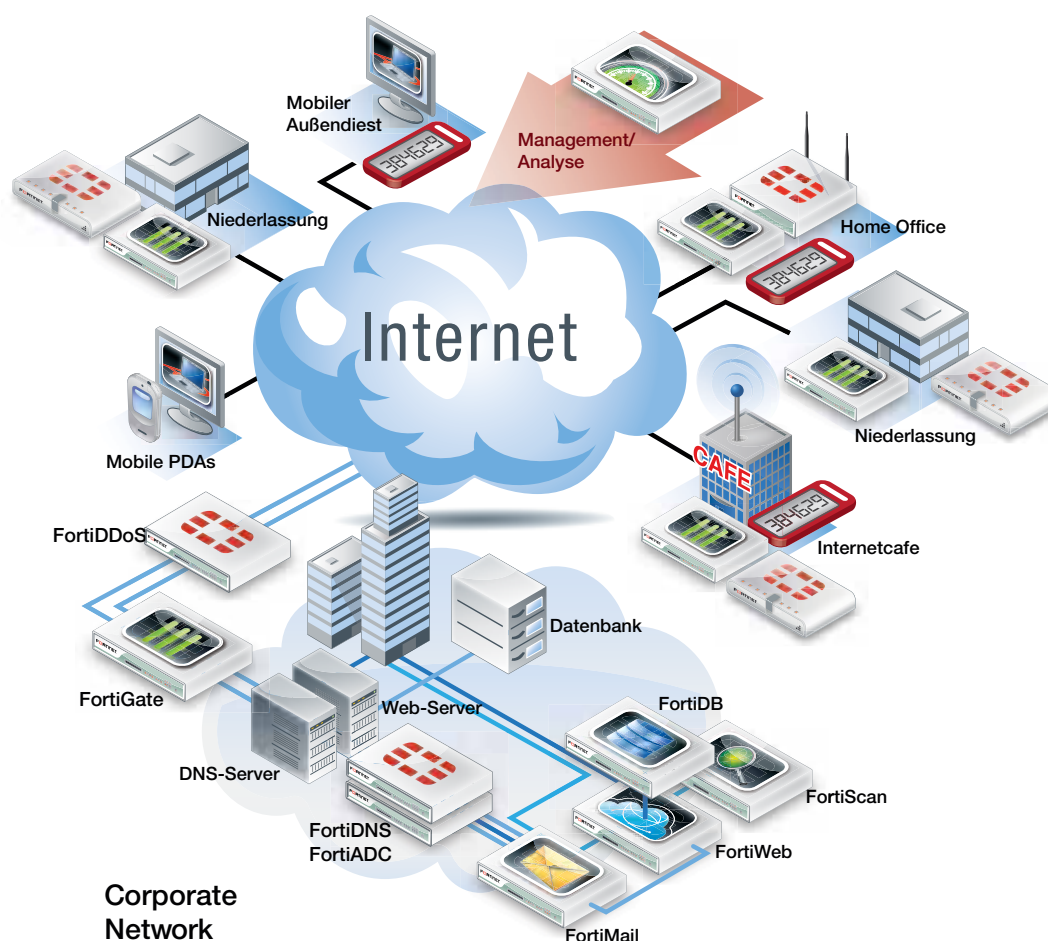
■ Einstiegslösungen

Sie benötigen umfassenden Unternehmensschutz für Ihre kleinsten Niederlassungen, Vertretungen, Ausrüstung am Kundenstandort und Einzelhandelsnetzwerke? FortiWiFi™ Geräte bietet den Vorteil, dass sie als „Thick Access Point“ fungieren und drahtlose Funktionen, mit denen Sie Ihren gesamten Traffic überwachen mit und ohne Kabel überwachen und steuern können. So vermeiden Sie die Kosten und potentiellen Sicherheitslücken eines separaten drahtlosen Netzwerks. Die optionale Power-Over-Ethernet (PoE)-Unterstützung der Einstiegslösungen von FortiGate beschleunigt und vereinfacht den Einsatz eines voll integrierten kabellosen Netzwerks.



■ Einsatzgebiete von Fortinet-Lösungen

Die Flexibilität der verschiedenen Fortinet-Lösungen und der ausschließliche Fokus auf IT-Sicherheit ermöglichen Unternehmen aller Größenordnungen die Implementierung ganzheitlicher, höchst leistungsfähiger und kostenoptimierter Security-Infrastrukturen. End-to-End-Security wird mit Fortinet-Produkte unkompliziert und kostengünstig realisierbar – in einzelnen, überschaubaren Projekt-Etappen, oder durch eine vollständige Migration mit vielen auf umfangreiche Rollouts abgestimmten Tools. Das Schaubild verdeutlicht die unterschiedlichen Einsatzmöglichkeiten, die von hochkomplexen Rechenzentren mit oder ohne Managed Services über kleine und große Unternehmens-Filialen, Home-Office-Absicherung, Mobile Security bis hin zu Remote-Access-Lösungen, Mail-Absicherung und Schutz von Web-Anwendungen reichen, um nur einige Wenige zu nennen.



Zielgruppen nach Größe:

- Nationale und internationale Großunternehmen
- Filialisten mit bis zu mehreren tausend Standorten
- Mittelständische Unternehmen
- Kleine Unternehmen

Ebenso können Fortinet-Produkte in allen Branchen optimal die Geschäftsprozesse absichern.

Zielgruppen nach Branche

- Automobil-Branche
- Bauunternehmen
- Behörden
- Bildungseinrichtungen
- Chemie & Pharma
- eCommerce (z. B. Online-Shops, eGaming, Portale u.v.m.)
- Einzel- und Großhandel
- Energieversorger
- Finanzunternehmen (Versicherungen, Banken)
- Gastronomie und Hotelgewerbe
- Gesundheitswesen
- Industrie
- Logistik
- Managed Security Service Provider
- Medien-Unternehmen
- Militär
- Produzierende Unternehmen
- Service Provider (xSPs)
- Stadtwerke
- Telekommunikations-Anbieter (Carrier)

■ FortiGate – High Performance Next Generation Firewalling

FortiGate Module

Fortinet bietet mit der Produktfamilie „FortiGate“ eine ganze Palette von mehrfach ausgezeichneten Appliances für den Schutz von Netzwerken und Applikationen. Die FortiGate Systeme schützen Daten zuverlässig und in Echtzeit vor Netzwerk- und Content-basierenden Bedrohungen.

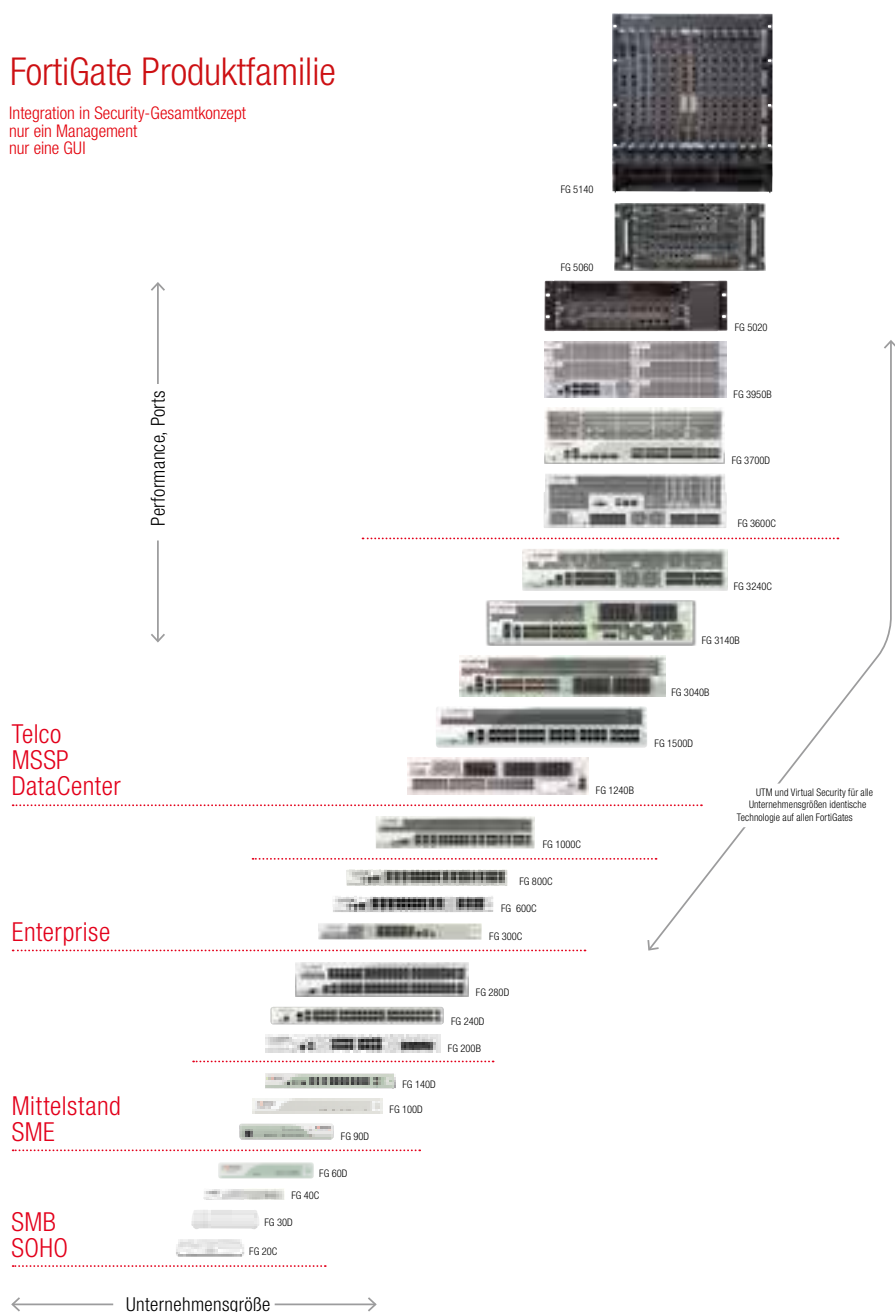
Hier spielen die von Fortinet entwickelten ASIC Prozessoren eine entscheidende Rolle, die die vielfältigen Dienste und Sicherheitsfunktionen der FortiGate Appliances enorm beschleunigen. Somit lassen sich Bedro-

hungen durch Viren, Würmer, Exploits, Spyware oder neuartige Blended Threats und Advanced Persistent Threats, also Kombinationen aus den genannten Angriffsmustern, effektiv bekämpfen – und das in Echtzeit!

Weitere Funktionen wie umfangreiche und komfortable Applikationskontrolle, URL-Filter, IPSec- und SSL-VPN, Bandbreitenmanagement, WLAN-Controller, integrierte 2-Faktor-Authentifizierung und selbstverständlich eine marktführende und hochperformante Firewall sind fest integrierter Bestandteil aller FortiGate Appliances.

FortiGate Produktfamilie

Integration in Security-Gesamtkonzept
nur ein Management
nur eine GUI



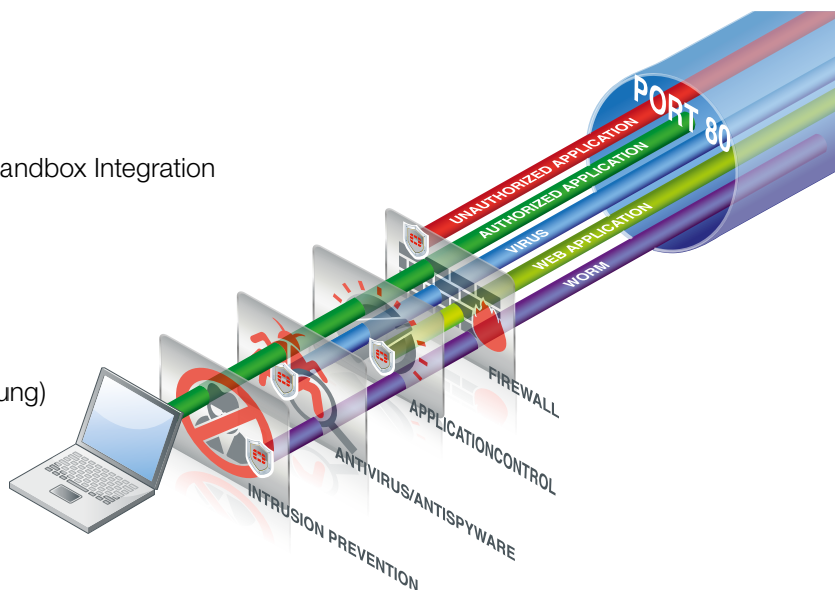


■ FortiOS – Das Sicherheits-Betriebssystem der FortiGate Serie

Das Betriebssystem aller FortiGate Systeme, FortiOS, bietet eine Vielzahl von Modulen, mit denen Unternehmen ihre Infrastruktur komfortabel und flexibel absichern können. FortiOS ist modular angelegt und kann mit späteren Updates im Rahmen eines bestehenden Service-Vertrages einfach um neue Funktionen erweitert werden – ohne zusätzliche Kosten!

Zur Zeit der Drucklegung dieser Broschüre beinhaltet FortiOS – und damit jede¹ FortiGate Appliance – folgende Funktionen:

- Firewall
- VPN
- AV
- IPS
- Advanced Threat Protection mit FortiSandbox Integration
- Applikationskontrolle
- URL-Filter
- Integrierter WLAN-Controller
- Integrierter Switch-Controller
- Mobile Security & BYOD (Client Reputation, Device/OS-Erkennung)
- WAN-Optimierung, Web-Cache & Explicit Proxy
- Authentifizierung via integriertem Token-Server
- Bandbreitenkontrolle
- IPv6-Support
- Data Loss Prevention
- SSL Inspection
- Smart Policies und Identity Based Policies
- Routing
- VLANs
- Virtuelle Instanzen (VDOMs)
- Endpoint Control – Integration FortiClient
- Skalierbares Security Management (optional via FortiManager)
- Umfangreiches Reporting und Troubleshooting (erweiterbar durch FortiCloud und FortiAnalyzer)
- FortiView – Monitoring und Troubleshooting “out of the box”



¹ FortiGate 20-50 verfügen z.T. über einen minimal eingeschränkten Funktionsumfang; s. Datenblatt

Die Module im einzelnen:

■ FortiGate Firewall

Die branchenführenden FortiGate Security-Systeme bieten unerreichte integrierte Security-Ressourcen, Benutzerfreundlichkeit und ein optimales Preis-Leistungsverhältnis. Zusammen mit der Stateful-Inspection-Firewall verwendet das FortiGate System eine Vielzahl an integrierten Sicherheitsmechanismen, um vor aktuellen und komplexen Angriffen, wie Stuxnet und Duqu effektiv zu schützen.

Das Herzstück aller FortiGate Modelle ist die schnellste Firewall der Welt (Quelle: Breaking Point). Firewall-Regelwerke kontrollieren sämtliche Daten, die eine FortiGate Appliance zu passieren versuchen – zwischen FortiGate Interfaces, Zonen oder VLAN-Sub-interfaces. Solche Regelwerke enthalten Anweisungen,

ob und wie einzelne Verbindungen akzeptiert oder Pakete weitergeleitet werden.

Bei Eintreffen einer Verbindungsanfrage werden z. B. Quell- und Zieladresse und der Dienst (Port Nummer) analysiert, um die anwendbaren Firewall-Regeln zu identifizieren. Dabei können u. U. viele verschiedene Instruktionen zur Anwendung kommen – neben obligatorischen Anweisungen wie dem Akzeptieren oder Verwerfen von Datenpaketen können optionale Instruktionen wie Loggen, Zuweisung von Bandbreite oder Authentifizierung greifen. Sämtliche anderen Sicherheitsmodule (z. B. AntiVirus, IPS, Applikationskontrolle, URL-Filter usw.) werden abhängig von diesem zentralen Firewall-Regelwerk gesteuert.

■ FortiGate VPN

Virtual Private Networks (VPN) ermöglichen die sichere, verschlüsselte Verbindung zu privaten Unternehmensnetzwerken und -ressourcen. So kann z.B. ein Anwender von seinem Home Office oder von unterwegs per VPN mittels einer verschlüsselten Verbindung auf das zentrale Netzwerk zugreifen. VPN-Verbindungen können nicht von unauthorisierten Dritten ausgelesen oder manipuliert werden und ein Zugriff auf sensible Informationen wird so verhindert.

Fortinet bietet VPN-Optionen, sowohl mittels seiner FortiGate Appliances, als auch über die in die FortiClient integrierte Funktionalität. Mittels zweier FortiGates (oder auch standard-konformen Drittanbietern) können auf diese Weise auch viele verschiedene Standorte sicher über ein VPN miteinander verbunden werden.

Hub and Spoke für Unternehmen

Hub-and-Spoke VPN-Konfigurationen ermöglichen, dass mehrere Fernstandorte miteinander verbunden werden können, ohne dass dabei spezielle Verbindungen für jeden Standort notwendig sind. Eine ideale Anwendung für diese Konzeption ist, den VoIP-Traffic

über VPNs zu transportieren, um so die Gebühren für Ferngespräche zu verringern. Fortinets Bandbreiten-Management-Funktionen ermöglichen, dass VoIP-Traffic auch bei einer VPN-Verbindung priorisiert wird.

SSL oder IPsec?

In den vergangenen Jahren haben sich zwei Standards für verschlüsselte Verbindungen etabliert: IPsec VPNs und SSL VPNs. Während IPsec VPNs primär in sog. site-2-site-Verbindungen und zentral gemanagten mobilen Endgeräten zum Einsatz kommen, haben sich SSL-VPNs vorwiegend in sog. clientless (z.B. Internet-Cafe) Umgebungen etabliert.

IPsec VPN bietet sich an für klassische Layer3-basierende Anwendungen, bei denen eine verschlüsselte Verbindung zwischen zwei Geräten aufgebaut wird. SSL VPN bietet Vorzüge im Bereich der Web-Anwendungen, bei denen zwischen Web-Server und Web-Browser eine sichere (SSL-verschlüsselte) Verbindung etabliert wird.

Fortinet unterstützt in höchst komfortabler Weise beide Standards und eine Vielzahl von Optionen zur individu-

ellen Konfiguration und Administration. Auf FortiGate Systemen können IPsec und SSL-VPN-Verbindungen auch gleichzeitig zum Einsatz kommen.

VPN-Services für MSSPs

Mit Fortinet können MSSPs einen hochsicheren VPN-Dienst bereitstellen, indem sie die integrierte VPN-Engine mit den übrigen UTM-Modulen verknüpfen. So kann ein- und ausgehender Traffic in Echtzeit auf Malware untersucht und erst dann freigegeben werden,

um die Verbreitung von Schadsoftware innerhalb eines Unternehmens-VPN zu verhindern.

Ein weiteres Plus ist, dass Fortinets flexible VPN-Architektur die Interoperabilität mit allen standardbasierten IPsec VPN-Gateways zulässt. Unabhängig vom VPN Device, das der Kunde verwendet, gewährleistet das zentral implementierte FortiGate System Malware-freien VPN Traffic.

FortiGate Intrusion Prevention Systeme (IPS)

Intrusion Prevention Systeme bieten Schutz gegen bekannte und zukünftige Bedrohungen auf Netzwerkebene. Zusätzlich zur Signatur-basierten Erkennung wird eine Anomalie-basierte Erkennung durchgeführt. Das System generiert einen Alarm, wenn Daten einem speziellen Profil eines Angriffsverhaltens entsprechen. Dieses Verhalten wird dann analysiert, um die Evolution von Bedrohungen zu erkennen und neue Signaturen entwickeln zu können, die dann wiederum Bestandteil der FortiGuard-Services werden.

Implementierung von IPS

Das in die FortiGate Appliances integrierte Hochleistungs-IPS-Modul kann entweder als Standalone-Device oder als Bestandteil einer Multifunktions-Firewall (UTM) sowie an Netzwerk-Perimeter (Übergang zwischen internem und externem Netzwerk) als auch im internen Netz agieren. So können sowohl protokoll- oder anwendungsbasierende Angriffe von außen als auch die Ausbreitung von derartigen Schädlingen im internen Netzwerk (die z. B. über mobile Endgeräte oder Datenträger ins Unternehmen gelangt sind) erkannt und verhindert werden.

IPS für die Zentrale und Niederlassungen

Fortinets flexible Architektur und skalierbare Produktreihe berücksichtigt Implementierungen im zentralen Netzwerkbereich zum Schutz vor externen und internen Angriffen ebenso wie die Absicherung von Niederlassungen jeder Größenordnung. Dies wird durch die identische IPS-Funktionalität auf allen FortiGate Appliances erreicht. In Verbindung mit FortiManager und FortiAnalyzer können so größte und hochkomplexe VPN-Infrastrukturen flexibel, einfach, kostengünstig und auch mandantenfähig realisiert werden.

One-Armed IDS (Sniffer)

Als Ergänzung ist es möglich, sog. Sniffer-Policies zu erstellen, mit denen eine FortiGate als „one-armed“ Intrusion Detection System fungiert, also nicht in den Datenstrom eingreift, sondern diesen nur mitliest. Dabei wird der Datenverkehr auf Übereinstimmungen mit bereits konfigurierten IPS-Sensoren und Applikationslisten untersucht. Bei einem Treffer wird dieser gelogged und die eingehenden Daten abgewiesen. Auf diese Weise ist es möglich, den Datenverkehr zu untersuchen ohne die einzelnen Datenpakete zu verarbeiten.

■ Fortigate (D)DoS-Abwehr

Typische Firewall-Systeme sind in der Lage, DoS- und DDoS-Angriffe zu erkennen, und sofern diese nur eine geringe Bandbreite belegen, auch abzuwehren. Dabei wird jedoch die CPU des Firewall-Systems stark belastet, da jedes angreifende Paket mithilfe einer Firewall-Regel bearbeitet werden muss. Fortinet bietet in seinen FortiGate Systemen ein mehrstufiges Abwehrmodell, welches die vorhandenen Ressourcen der Appliance deutlich entlastet.

DoS-Sensor

Mithilfe eines sogenannten DoS-Sensors können DoS-Angriffe bereits erkannt werden, bevor klassische Firewall-Regeln greifen. Der DoS-Sensor, der viele verschiedene Typen von Netzwerk-Anomalien erkennen kann, unterscheidet zwischen angreifenden und erlaubten Daten. Erlaubte Daten werden an das Regelwerk der Firewall übergeben, Pakete die als DoS-Angriff gewertet werden, werden entsprechend der im DoS-Sensor hinterlegten Konfiguration behandelt. Nachgeschaltete Intelligenz in einem FortiGate System, wie etwa die IPS Engine, bietet darüber hinaus weitere Möglichkeiten zur Erkennung von DoS- und DDoS-Angriffen auf höheren Netzwerkschichten.

■ FortiGate Applikationskontrolle

Die Vielfalt von Applikationen nimmt kontinuierlich und zum Teil sogar drastisch zu – verstärkt durch den Trend, dass Enterprise-Applikationen zunehmend in Richtung Web-Plattformen migrieren und Web 2.0 mit einer Vielzahl von einfachen und vielfach privat genutzten Anwendungen (Webmail, Instant Messaging, Social Media wie Twitter und Facebook usw.) den Administratoren das Leben erschwert.

Daraus ergeben sich neue Herausforderungen für die IT-Sicherheit, da vielen dieser Anwendungen neue Sicherheitslücken innewohnen, die herkömmliche Abwehrmaßnahmen umgehen können. Desweiteren stehen IT-Verantwortliche vor dem Problem, die Produktivität der Mitarbeiter trotz derartiger oft zeitintensiver Applikationen (Chat, Games usw.) zu erhalten und die Zuverlässigkeit der Infrastruktur zu bewahren, obwohl diese Anwendungen oft eine sehr hohe Bandbreite

Hardware basierte DoS-Abwehr

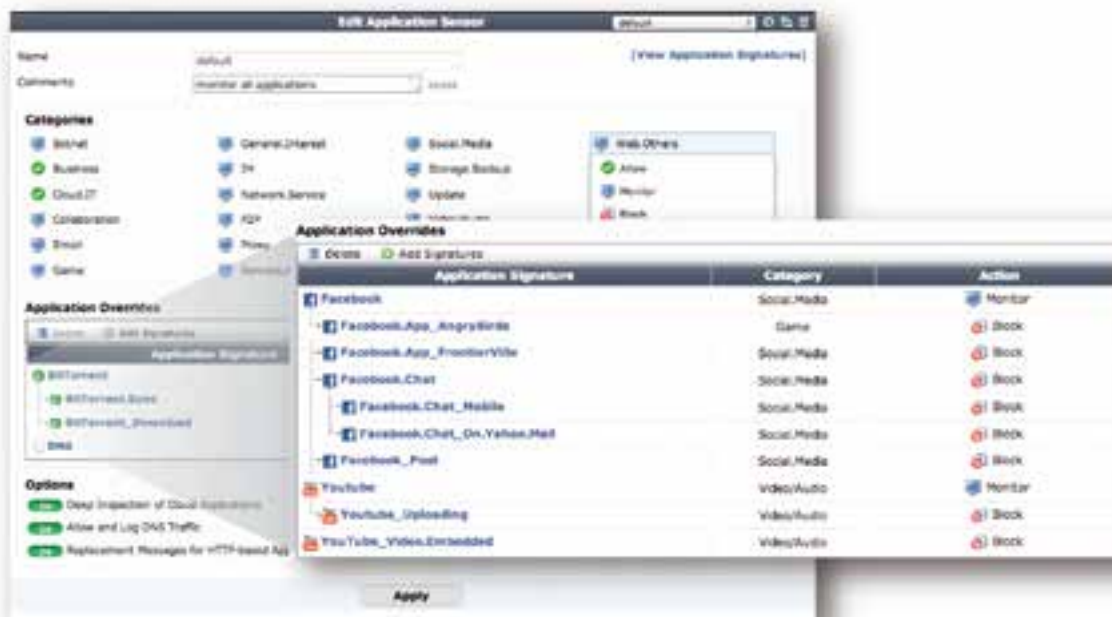
Mithilfe der Fortinet ASICs SP2 oder SP3, die in einigen größeren FortiGate Appliances sowie Erweiterungsmodulen integriert sind, kann mittels der dort vorhandenen Proxyfunktionalität eine TCP SYN Flood Attacke erkannt und abgewehrt werden, ohne die restliche Appliance-Architektur nennenswert zu belasten. Durch die im SP3 integrierten Load Balancer-Funktionen ist es sogar möglich, hochperformante DDoS-Abwehr parallel zur ebenso leistungsfähigen IPS-Funktionalität zu betreiben, indem die Daten entsprechend auf weitere interne Module bzw. Prozessoren (ASICs) verteilt werden.

In modularen FortiGate Appliances können zu diesem Zweck sog. Security Processing-Module nachgerüstet werden, die mit den neuen SP2/SP3-Chips ausgestattet sind. So kann (bei Bedarf auch erst im Nachhinein) die IPS-Performance einer Appliance signifikant gesteigert werden.

benötigen (Video/Audio-Downloads oder -Streaming). Zunehmend spielt auch die Einhaltung von Compliance-Regularien eine Rolle, die weitere Anforderungen an IT-Abteilungen stellt.

Arbeitsweise

Applikationskontrolle stellt ein Werkzeug zur Verfügung, das Administratoren in die Lage versetzt, gezielt auf einzelne Applikationen einzuwirken – auch dann, wenn diese Non-Standard Ports verwenden oder erlaubte Protokolle als Tunnel nutzen. Als Teil einer Multi-Layer-Security-Architektur ermöglicht Applikationskontrolle eine granulare Steuerung des Anwendungsverhalten und beeinflusst so im positiven Sinne die Bandbreite, Performance, Stabilität und Zuverlässigkeit sowie die Compliance der IT-Infrastruktur.



Vorteile gegenüber herkömmlichen Methoden

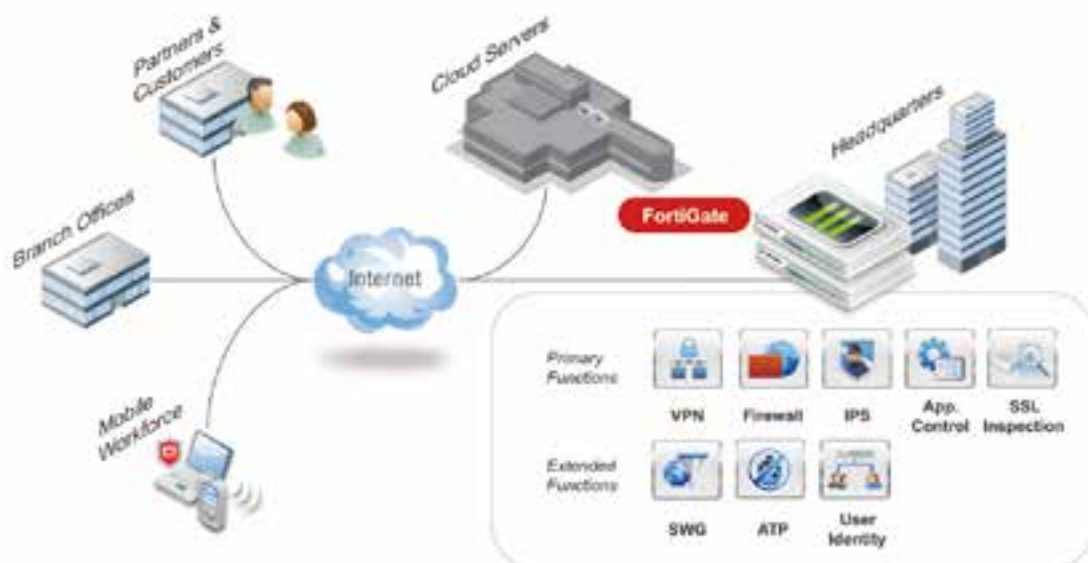
Eine herkömmliche Firewall kontrolliert den Datenstrom basierend auf Port- bzw. Service-Kontrollmechanismen. Applikations-Kontrolle setzt auf dynamische Untersuchung der Daten und ermöglicht überdies die Anwendung weiterer Kontrollen, wie etwa Bandbreitenvergabe pro Applikation oder Zeitfenster bzw. -konten für deren Nutzung. Weiterhin kann sogar innerhalb von Applikationen ein Teil der Funktionalität eingeschränkt werden, z. B. die Nutzung von Facebook bei gleichzeitigem Unterbinden von Facebook Chat, oder das Nutzen von Google.Docs, oder aber das Unterbinden von Google.Talk.

Applikations-Kontrolle ergänzt somit die Funktionalität von Firewall- und IPS-Mechanismen um eine granulare Steuerung von Anwendungen und Protokollen. Die maximale Nutzbarkeit von Applikationen wird so bei minimalem Risiko erzielt. Derartige Regeln zur Nutzung können bis auf Anwenderebene und selbstverständlich auch geräte- oder abteilungsbezogen erstellt werden.

Integration als Mehrwert

Es ist wichtig, Applikations-Kontrolle nicht als isolierten Bestandteil der IT-Sicherheit zu verstehen, denn dies führt zu einem reaktiven Ansatz der Security-Strategie. Vielmehr ergänzt es sinnvoll die vorhandenen Abwehrmechanismen wie z.B. Firewall, VPN, AntiVirus, IPS und Web Filter, und idealerweise integriert es sich in diese. Unternehmen leiden zunehmend an der – nicht nur in IT-Security-Umgebungen – häufig anzutreffenden viel zu heterogen gewachsenen Struktur, die auf sog. Point-Solutions, also Nischen-Lösungen basieren. Diese integrieren sich nur bedingt oder gar nicht, sind aufgrund der Vielfalt schwierig in der Administration und erhöhen oft unbemerkt die Betriebskosten eines Unternehmens in beträchtlicher Weise.

Als unangenehmen Nebeneffekt beeinflussen solche oft seriell in einen Datenstrom eingebrachten Lösungen auch die Gesamt-Performance des Netzwerks negativ, da durch diese Vorgehensweise Pakete oft mehrfach analysiert werden – oder im schlimmsten Fall sogar Paketinformationen für eine sinnvolle Analyse gar nicht mehr zur Verfügung stehen.



■ FortiGate AntiVirus

Das Antivirus-Modul vereint eine Reihe von Features, die verhindern, dass ungewollte oder potenziell gefährliche Dateien in das Netzwerk gelangen. Diese Features arbeiten auf unterschiedliche Weise, wie etwa das Prüfen der Dateigröße, des Namens, des Dateityps, oder des Vorhandenseins eines Virus oder einer Grayware Signatur. Dabei haben alle Antivirus-Mechanismen gleichzeitig Zugriff auf den Datenverkehr, wodurch sichergestellt ist, dass viele Operationen nahezu gleichzeitig erfolgen können. Dies erhöht die Performance der Antivirus-Engine erheblich.

Proxy-, Flow- oder Cloud-basierter AntiVirus

Zusätzlich zu drei Proxy-basierenden Antivirus-Datenbanken beinhaltet FortiOS außerdem eine hoch performante flow-basierende Antivirus-Option. Diese ermöglicht es, Dateien jeder Größe zu scannen, ohne die Performance merklich zu beeinträchtigen. Überdies ist es möglich, komprimierte Dateien zu analysieren um auch versteckte Threats zu erkennen. Durch die Flexibilität, zwischen den Antivirus-Engines wählen zu können, ist es möglich, die ideale Ausgewogenheit zwischen Performance und Security individuell an die Umgebung anzupassen.

Ab FortiOS 5 steht darüber hinaus eine Cloud-basierte AV-Engine zur Verfügung. Diese ergänzt die zuvor ge-

nannten Engines und bietet zusätzliches Sandboxing. So können – ohne die Performance der FortiGate zu beeinträchtigen – Dateien in der Cloud analysiert und ihre Gefährlichkeit in einer sog. Sandbox geprüft werden.

High Performance AntiVirus

Fortinets optimierte Anti-Virus-Technologie verwendet eine Kombination aus Signatur- und heuristischen Detektionsmodulen und bietet so vielschichtigen Echtzeitschutz gegen zahlreiche Angriffsformen. Extrem hohe System-Performance wird durch die Verwendung des integrierten FortiASIC Content-Prozessors (CP) zusammen mit Fortinets patentierter Technologie, bekannt unter der Bezeichnung CPRL oder Content Pattern Recognition Language, erreicht, die dem beschleunigten Scannen von Virusdateien und der Heuristik/Anomalie-Erkennung dienen.

AntiVirus Techniken

Abhängig vom erforderlichen Schutzniveau können unterschiedliche Instanzen aktiviert werden, die eingehende Daten auf Malware untersuchen. Dabei wird unterschieden zwischen Pattern Scan, Grayware Scan und einer heuristischen Analyse. Während die ersten beiden Verfahren auf bekannte Virus-Definitionen untersuchen, ist es möglich, mit Letzterer auch Mutationen bekannter Viren oder gänzlich neue Viren-Signaturen zu erkennen.

Echtzeit Updates

Die Effizienz einer Antivirus-Lösung wird nicht nur an ihrem Durchsatz oder an der Erkennungsrate, sondern auch an der Geschwindigkeit, in der Signatur-Updates eintreffen, gemessen. Über das FortiGuard Distribution Network (FDN) werden diese Informationen kontinuierlich aktualisiert und in Echtzeit bereitgestellt. Dieser Vorgang erfolgt automatisch und erfordert keinen Eingriff des Administrators. Im Vergleich rangiert die Fortinet AV-Engine kontinuierlich unter den Top5 AntiVirus-Anbietern.

Advanced Threat Protection – Integration in FortiSandbox

Moderne, hochgradig komplexe und „hartnäckige“ Malware ist nicht selten so programmiert, dass sie Wege

zu finden versucht, vorhandene Abwehrmechanismen wie Firewall, AV, IPS usw. zu umgehen. An dieser Stelle greifen weitere Erkennungsmethoden und die Integration einer FortiGate mit Fortinets Sandbox-Technologie. Verdächtig wirkende Daten werden – bevor sie ins Unternehmensnetz gelangen können, an eine FortiSandbox weitergeleitet. Dort werden sie in einer isolierten Umgebung zur Ausführung gebracht und auf ihre Wirkung untersucht.

Sollte dabei ein schadhaftes Verhalten erkannt werden, werden die Daten geblockt und das Ergebnis der Analyse an die Fortinet Labs gesendet, die daraufhin neue Signaturen entwickeln und bereitstellen. Weitere Informationen zu Fortinets Sandbox-Lösungen finden Sie im gleichnamigen Kapitel in dieser Broschüre.

■ FortiGate Web-Filter

Unerlaubtes Internet-Surfen und die Verwendung von webbasierenden Anwendungen resultieren häufig in Produktivitätsverlust, hoher Netzwerklast, Infizierung mit Malware und Datenverlusten. Web Filtering kontrolliert den Zugriff auf webbasierte Anwendungen wie Instant Messaging, Peer-to-Peer File Sharing und Streaming-Applikationen. Gleichzeitig werden Phishing Sites und Blended Threats blockiert. Überdies können Botnet Befehle und Fast Flux File Downloads blockiert werden. Flowbasierende Web Filtering Optionen sind ebenfalls verfügbar.

Arbeitsweise

Das Fortinet WebFilter-Modul besteht aus drei interagierenden Komponenten: dem URL-Filter, dem Web Content Filter und dem FortiGuard Webfilter Service. Der URL-Filter verwendet URLs und URL Patterns, um Webseiten zu blockieren. Der Web Content Filter blockiert Webseiten, die bestimmte Wörter oder Patterns

enthalten, die individuell spezifiziert werden können. Fortinets FortiGuard Web Filtering Service reguliert und bietet wertvolle Einsicht in alle Internetaktivitäten und ermöglicht es dem Kunden so, neue gesetzliche oder interne Bestimmungen und Vorschriften einzuhalten.

Jugendschutz

Fortinet ist ein Mitglied der Internet Watch Foundation in Großbritannien, eine Organisation, die potenziell illegalen Online-Content bekämpft und den Zugang zu kinderpornografischen Websites verhindert. Fortinets Web Filtering Lösungen sind darüber hinaus CIPA-zertifiziert. Das Children's Internet Protection Act (CIPA) ist ein US-Bundesgesetz, das im Dezember 2000 vom amerikanischen Kongress verabschiedet wurde, um Problemen hinsichtlich des Zugangs auf das Internet und andere Informationen in Schulen und Bibliotheken entgegenzusteuern.

■ FortiGate Secure WLAN

FortiGate Security-Systeme bieten eine umfassende Reihe an Funktionen, mit denen die höchsten Anforderungen bei der Implementierung von Wireless LANs erfüllt werden. FortiGate Systeme können in Verbindung

mit Wireless Access Points (FortiAP) implementiert und dazu verwendet werden, Content-basierte Bedrohungen aus E-Mail- und Internet-Traffic, wie Viren, Würmer, Intrusionen, unangemessenen Internet Content, in



Echtzeit zu ermitteln und zu eliminieren, ohne dabei die Performance des Netzwerkes zu beeinträchtigen.

Neben der Bereitstellung von anwendungsbezogenem Schutz bieten die FortiGate Systeme umfassende netzwerkbezogene Dienste, wie Firewall, VPN, Intrusion Detection und Bandbreitenmanagement, welche einen vollständigen Netzwerkschutz-Service mittels spezieller, leicht zu verwaltender Plattformen bieten. Insbesondere VPN Verschlüsselungs-, Anwender-Authentifizierungs- und Dateiverzeichnis-Integrations-Leistungsmerkmale der FortiGate Systeme ermöglichen eine Eindämmung von Sicherheitslücken von WLAN-Produkten der jetzigen Generation und bieten eine vollständige Nachrüstung für jede WLAN-Implementierung.

Die umfangreiche Serie von Fortinet-eigenen Thin Access Points (FortiAP) in Verbindung mit einer Vielzahl von Wireless Controllern (FortiGate Appliances ab FortiOS 4.1.) bietet High-Performance Netzwerkzugänge mit integrierter Content-Security. Durch die Kombination eines Wireless Controllers mit einer FortiGate Plattform (größer als Modell FG30B) wird das Sicherheitsniveau des kabelgebundenen LANs automatisch auf die WLAN Umgebung übertragen.

Der gesamte WLAN-Traffic wird so Identitäts-basiert über die UTM-Engines der FortiGate Appliance geleitet und dort entsprechend analysiert, und es werden nur autorisierte Verbindungen zugelassen. Durch diese Integration ist es möglich, von einer einzigen Konsole

aus den Netzwerkzugang zu überwachen, Regelwerke einfach und schnell upzudaten und den Datenverkehr und die Einhaltung von Compliance-Regeln kontinuierlich zu prüfen.

Return on Investment

Da jede FortiGate Appliance (ab FG40C) ab FortiOS 4.3. über diese Wireless-Controller-Funktionalität verfügt, können bereits bestehende Gateways durch ein einfaches Betriebssystem-Update um dieses Feature erweitert werden – die Anschaffung einer zusätzlichen Plattform mit einer eigenen Administrations-Oberfläche entfällt.

Durch die hohe Performance und große Reichweite der neuen FortiAP Serie ist der Aufbau einer hochsicheren und leistungsstarken WLAN-Infrastruktur einfach und kostengünstig möglich. In vielen Anwendungsszenarien erübrigt sich unter Umständen sogar das Installieren einer Verkabelung bis zum Arbeitsplatz, da die Durchsatzraten der WLAN-Lösung vielfach äquivalent hoch sind.

Access Points für alle Anwendungen

FortiAPs stehen für alle denkbaren Anwendungen zur Verfügung. Indoor, Outdoor, Remote Access Points sowie umfangreiches Zubehör wie z.B. verschiedene Antennen finden sich im entsprechenden Kapitel dieser Broschüre.

■ FortiGate Mobile Security und BYOD (Bring Your Own Device)

Die drastische Zunahme von mobilen Endgeräten, die z. T. auch Privateigentum der Nutzer sind, stellt Unternehmen vor eine neue Dimension an Herausforderungen: Kontrolle über Geräte, auf die aufgrund der Gesetzeslage kein, oder nur ein stark beschränkter und vor allem reglementierter Zugriff möglich ist. Aber auch, wenn die Endgeräte Unternehmenseigentum sind, ist eine sichere Kontrolle oft nur bedingt möglich (z. B. bietet das iOS der Apple-Welt kaum Möglichkeiten, Security-Software zu installieren). Hier müssen zentrale Mechanismen die dezentrale Sicherheit schaffen.

Device- und OS-Erkennung

Ab FortiOS 5 stellen alle FortiGate Appliances umfangreiche Funktionen für diesen Zweck bereit. So können anhand spezieller Parameter die Endgeräte (Typ & Hersteller) sowie die installierten Betriebssysteme (Typ & Release) erkannt werden. In Verbindung mit geographischer Ortsbestimmung, User-Erkennung und -Authentifizierung und ggf. weiterer Eckdaten (Zeit, Datenmenge, Ressourcen etc.) sind so individuelle Regelwerke möglich, die in Abhängigkeit dieser Rahmenparameter herangezogen werden können.

■ FortiGate Client Reputation

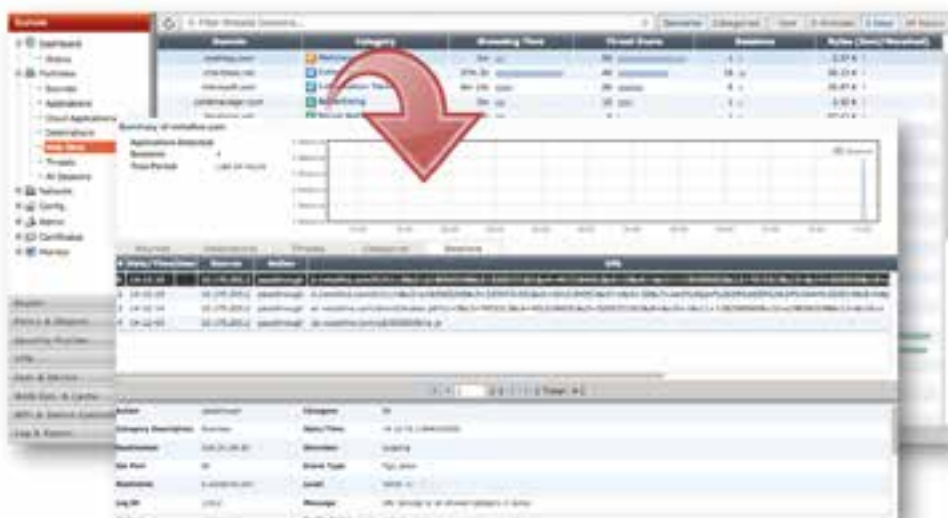
Nicht nur in BYOD-Umgebungen, sondern in jedem Unternehmen ist es wichtig, frühzeitig zu erkennen, welche User bewusst oder unbewusst die IT-Sicherheit gefährden. Dies kann durch Nutzung unerlaubter Software, Surfen auf gefährlichen Webseiten oder Download von infizierten Dateien (Bilder, PDFs, Audio, Video) erfolgen – aber auch durch die unbemerkte Infektion durch Zombie-Code, der das Endgerät zum Teil eines Botnets macht.

Die neue FortiOS Client Reputation Funktionalität erlaubt es, Usern individuelle Nutzungsprofile zuzuweisen, diese regelmäßig auf Abweichungen zu scannen und so eine Nutzer-ScoreCard anzulegen. Diese dient

wiederum als Basis für Regelwerke, die in Abhängigkeit des User-Scores adaptiert werden können bzw. Alarme auslösen.

FortiGate Monitoring und Troubleshooting mit FortiView

Mit FortiView, einem ab FortiOS 5.2. verfügbaren integrierten Tool zum Monitoring und Troubleshooting, ist es nunmehr möglich, schnell und einfach die Events einer FortiGate zu visualisieren und die Fehlersuche deutlich zu vereinfachen. Detaillierte Logs bieten tiefen Einblick in Sessions einer FortiGate, umfangreiche Reports optimieren und erleichtern die vorausschauende Netzwerkplanung.



■ FortiGate Virtuelle Instanzen

Die Konsolidierung unterschiedlicher IT-Security-Dienste auf einer einzigen Hardware-Plattform kann durch deren Virtualisierung optimal ergänzt werden. So lassen sich Kosten senken, die sonst aufgrund von hohem Platzbedarf, aufwändiger Wartung und Bedienung, komplizierter Verwaltung von Service-Verträgen, Stromverbrauch und mangelhafter Flexibilität entstehen würden. Darüber hinaus benötigen immer mehr Unternehmen heterogene Security-Dienste für einzelne Teile ihrer Infrastruktur, also unterschiedliche Funktionen für verschiedene Abteilungen.

Virtuelle Domänen (VDMs)

Mit der standardisierten und integrierten Virtualisierungsfunktion – sogenannten virtuellen Domänen (VDMs) – können sämtliche Funktionen einer FortiGate Appliance auch als virtuelle Einheit abgebildet werden. Daraus ergibt sich die Möglichkeit, dass einzelne Abteilungen oder Kunden mehrere oder auch nur bestimmte Funktionen wie Firewall, AV- oder IPS-Dienste nutzen können. Die Verwaltung läuft dabei auf ein und derselben Appliance.

Bei allen FortiGate Modellen sind 10 VDMs möglich und ab Werk ohne zusätzliche Kosten vorhanden. Ab der 1000er Serie sind mit zusätzlichen Lizenzen weitere VDMs pro FortiGate möglich. Neben vielen äußerst

flexiblen Konfigurations-Optionen reduziert der Einsatz von VDMs auch den Platz- und Strombedarf. So können z.B. mit einer einzigen FG600C bis zu 10 kleinere FortiGates (z.B. FG40C oder FG60D) ersetzt werden – ein deutlicher Platzvorteil und bis zu 18.000 kWh Stromersparnis pro Jahr.

Höchste Flexibilität

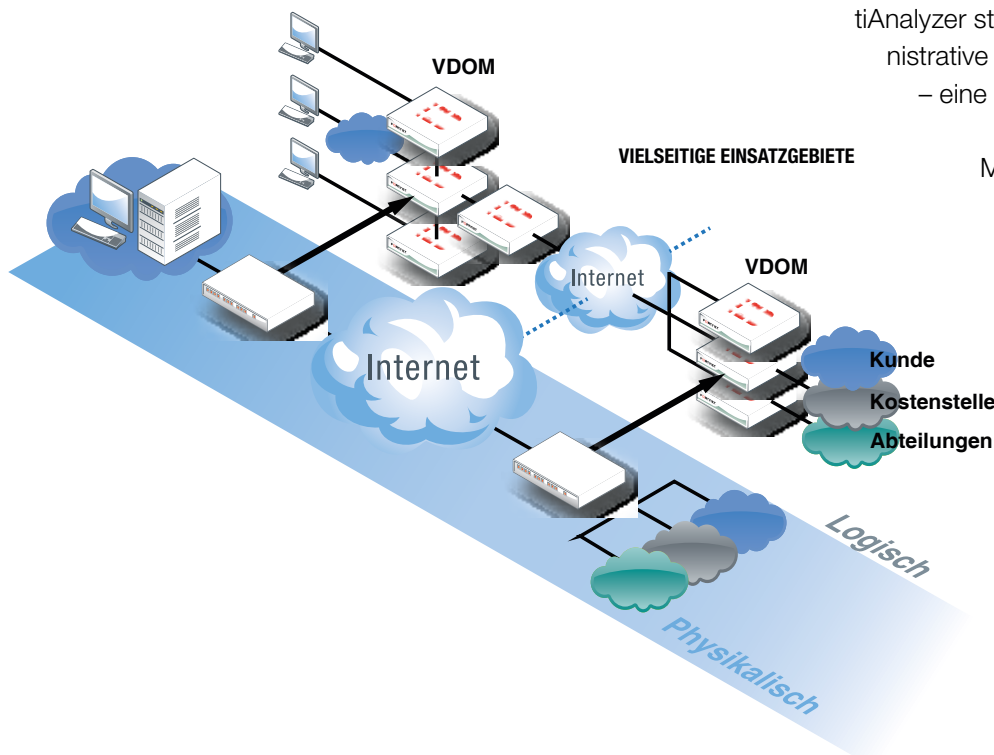
VDMs ermöglichen nicht nur individuelle Security-Service-Konfigurationen innerhalb von Unternehmen oder für MSSPs. Sie bieten weitere Vorteile, wie z.B. die optimierte Lastverteilung innerhalb eines Clusters, in dem auf einem Cluster-Member z. B. die Firewall im Primary- und die AV-Engine im StandBy-Modus ausgeführt wird – und im anderen Cluster-Member entsprechend umgekehrt. So wird die Performance beider Appliances optimal genutzt und trotzdem eine Hochverfügbarkeit gewährleistet. Ebenso kann auf diese Weise ein Cluster entsprechend skaliert werden, ohne dass Geräte ausgetauscht werden müssten.

Mandantenfähige Security Services

In Verbindung mit FortiManager und FortiAnalyzer können extrem flexible Management- und Reporting-Funktionen mandantenfähig abgebildet und entweder durch den Kunden, die Abteilung oder den Dienstleister verwaltet werden. Sowohl FortiManager als auch FortiAnalyzer stellen diese Funktionalitäten, sog. Administrative Domains (ADOMs), standardmäßig bereit – eine Erweiterung ist hier nicht erforderlich.

MSSPs können auf diese Weise sehr einfach und kostengünstig maßgeschneiderte Security Services anbieten.

Dabei kann jede einzelne VDM individuell und völlig unabhängig mit dem vollen Funktionsumfang einer FortiGate konfiguriert werden. Änderungen sind ebenso einfach und schnell – und vor allem ohne Unterbrechung der Services möglich. Ebenso kann eine Inter-VDM-Kommunikation etabliert werden, wenn dies aus Kundensicht oder für administrative Zwecke erforderlich sein sollte.



■ FortiGate 2-Faktor-Authentifizierung mit FortiToken

Bei der Authentifizierung handelt es sich um die Bestätigung der Identität von Personen oder Instanzen. Im Zusammenhang mit Unternehmensnetzwerken müssen die Identitäten von Nutzern oder Computern definiert und kontrolliert werden, um sicherzustellen, dass nur autorisierte Instanzen Zugriff auf das Netzwerk bekommen.

Fortinet Systeme unterstützen Netzwerk Zugangskontrolle (NAC) und können so Firewall-Regeln und VPN-Dienste einzelnen Usern dediziert zuweisen. Eine FortiGate Appliance unterstützt drei unterschiedliche Authentifizierung-Methoden: Passwort-Authentifizierung für Personen, Zertifikat-basierende Authentifizierung für Host-Computer oder Endpoints, sowie 2-Faktor-Authentifizierung für zusätzliche Sicherheit über normale Passwörter hinaus.

Lokale Passwortauthentifizierung

Die einfachste Möglichkeit der Authentifizierung basiert auf User-Accounts, die bereits lokal auf einer FortiGate Appliance gespeichert sind. Über die Möglichkeit, einen User-Account vorübergehend abzuschalten, ist es möglich, den Netzwerkzugang zu unterbinden, ohne den Account zu löschen. Lokale User-Accounts sind eine gute Methode für kleinere FortiGate Installationen. Sobald mehrere FortiGate Appliances zum Einsatz kommen, die mit denselben Accounts arbeiten, ist die Verwendung externer Authentifizierungsserver empfehlenswert, um die Account-Verwaltung und -Konfiguration zu vereinfachen.

Server-basierter Passwortauthentifizierung

Die Nutzung von externen LDAP, RADIUS oder TACACS+ Authentifizierungs-Servern ist immer dann wünschenswert, wenn mehrere FortiGate Appliances dieselben Anwender authentifizieren müssen, oder wenn eine FortiGate in ein Netzwerk integriert wird, das bereits einen Authentifizierungsserver beinhaltet.

Single Sign On mittels FSAE

„Single (user) Sign On“ bedeutet, dass sich Anwender nur einmal anmelden müssen, um auf unterschiedliche Netzwerkressourcen zugreifen zu können. Die Forti-

net Server Authentication Extension (FSAE) bietet u.a. Single Sign On Möglichkeiten für:

- Microsoft Windows Netzwerke mit Active Directory oder NTLM Authentifizierung
- Novell Netzwerke mit eDirectory
- Zertifikat-basierte Authentifizierung

Ein RSA X.509 Server Zertifikat ist eine kleine Datei, die von einer Certificate Authority (CA) ausgegeben wird, die entweder auf einem Computer oder auf einer FortiGate Appliance installiert ist, um sich selbst gegenüber anderen Geräten innerhalb des Netzwerks zu authentifizieren. Wenn sich nun eine Instanz im Netzwerk mittels eines Zertifikates authentifiziert, kann die andere Instanz prüfen, ob dieses Zertifikat von der CA ausgegeben wurde. Die Identifizierung ist daher so vertrauenswürdig, wie die CA, die das Zertifikat ausgegeben hat. Zum Schutz gegen modifizierte oder missbräuchlich genutzte Zertifikate ist es möglich, diese von der CA zurückrufen zu lassen.

2-Faktor Authentifizierung

Optional und zur Erhöhung der Sicherheit kann ein User aufgefordert werden, zusätzlich zu bekannten Informationen (Usernamen und Passwort) einen speziellen Besitz (FortiToken oder Zertifikate) zu dokumentieren. Bei einem FortiToken handelt es sich um einen Code Generator, der für die Authentifizierung einen einmaligen Code generiert. Wenn dieses Feature aktiviert ist, muss der Anwender zusätzlich zu Username und Passwort diesen Code eingeben.

Die FortiGate Appliance verifiziert dann den Code des FortiToken in Kombination mit Usernamen und Passwort. Diese Form der Authentifizierung kann z.B. für den Aufbau einer VPN-Verbindung, für den Administration-Zugang oder die Nutzung eines WLAN-Portals verwendet werden. Als weitere Optionen für diese Art der Authentifizierung stehen der Versand einer E-Mail oder einer SMS an den sich anmeldenden User zur Verfügung. In diesem Fall müssen die darin enthaltenen Codes zusätzlich zur Anmeldung eingegeben werden.

■ FortiGate Data Loss Prevention

Der ungewollte oder mit krimineller Energie gezielte Versand sensibler Daten erzeugt nicht nur hohe Kosten, sondern kann auch das Image eines Unternehmens stark beschädigen. Data Loss Prevention (oder DLP) bezeichnet ein System oder eine Software, die zuvor definierte vertrauliche Daten identifiziert, monitort und deren unerwünschten Versand verhindert.

Die in FortiOS integrierten DLP Features beinhalten Finger Printing von Dokumenten oder deren Quellen, verschiedene Inspektionsmodi, erweitertes Pattern Matching sowie Datenarchivierung. Nahezu sämtliche

Inhalte können analysiert werden, darunter auch HTTP, HTTPS, FTP, FTPS, E-Mail (POP3, POP3S, IMAP, IMPS, SMTP, SMTPS), NNTP und Instant Messaging (AIM, ICQ, MSN und Yahoo!) Protokolle.

Hierbei können Textvergleiche ebenso wie erweitertes Pattern Matching mittels Wildcards oder Perl-Ausdrücken erfolgen. Zum Beispiel kann durch voreingestellte Pattern der Versand oder Empfang von Kreditkartennummern erkannt, gemeldet und/oder blockiert werden.

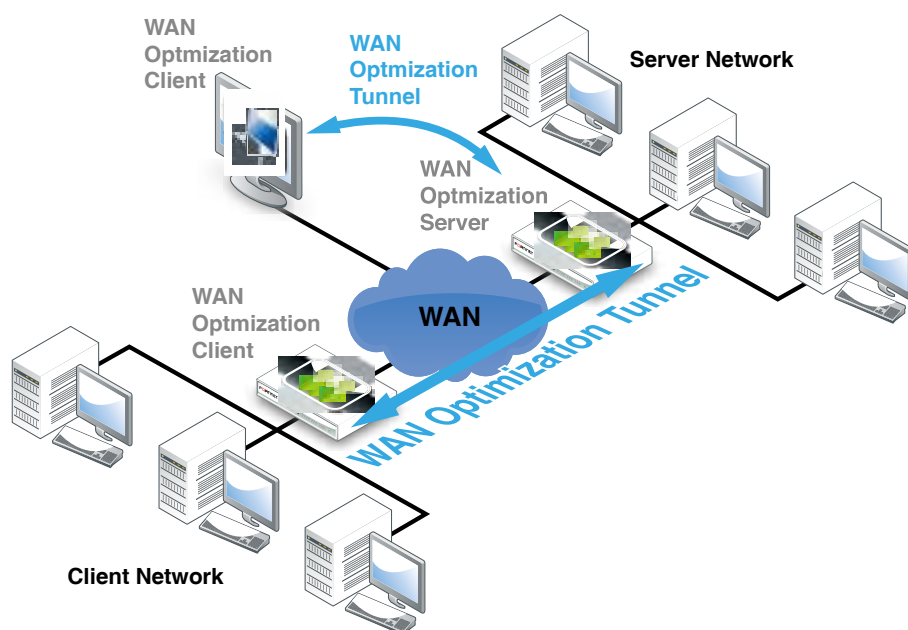
■ FortiGate WAN-Optimierung

Bedingt durch die Zentralisierung von Applikationen oder Serverfarmen ebenso wie die verstärkte Nutzung von Cloud Services rückt das Thema Bandbreite auf WAN-Verbindungen verstärkt in den Mittelpunkt. Häufig sind gerade kleinere Niederlassungen nicht mit hoher Bandbreite angebunden. Applikationen, die ursprünglich für die Nutzung in lokalen Netzwerken entwickelt wurden, werden in die Cloud verschoben und verursachen nun eine drastische Zunahme des Datenverkehrs auf den WAN-Verbindungen.

Anwendungen wie Windows File Sharing (CIFS), E-Mail (MAPI) und viele andere Applikationen erreichen auf diese Weise bei weitem nicht mehr die Performance, die sie in lokalen Netzwerken auszeichnen. Das Ergebnis sind häufig Produktivitätsverlust, kostspielige Netzwerk-Upgrades, teurere WAN-Verbindungen und eine höhere Belastung des IT-Personals.

Die FortiOS WAN-Optimierung beschleunigt den WANZugriff auf Applikationen und sorgt gleichzeitig für die Sicherheit der Verbindungen. Der Service sorgt

für mehr Performance, Produktivität und Bandbreiten-Reduzierung, verbesserte Server-Ressourcen und geringere Netzwerkkosten. Mit Protokolloptimierung, Byte Caching, Web & File Caching sowie SSL-Beschleunigung stehen verschiedene Tools bereits, die die benötigte Bandbreite drastisch – um bis zu 80% – reduzieren können.



■ FortiGate AntiSpam

Fortinet Anti Spam-Technologie bietet umfangreiche Möglichkeiten Spam Mails zu erkennen und zu blockieren. In gleicher Weise werden schadhafte Mail-Anhänge zuverlässig erkannt, um Angriffe von SpamBots und kompromittierten Systemen abzuwehren. FortiGate und FortiWifi-Plattformen bieten integrierte AntiSpam Funktionalität als Teil ihrer Multi Layer Schutzmechanismen. Diese werden durch kontinuierliche FortiGuard Update Services aktualisiert.

Die in FortiGate Systemen integrierte AntiSpam-Technologie kann – je nach Infrastruktur und Datenaufkommen, insbesondere bei kleineren Unternehmen eine völlig ausreichende Spam-Abwehr darstellen. Mails werden hier zwar nicht quarantänisiert (diese Funktion und viele andere bieten FortiMail Systeme – s. dazu entsprechendes Kapitel in dieser Broschüre), aber mit einer bereits sehr hohen Erkennungsrate aufgrund von Reputations-Analyse geblockt und belasten damit die internen Mail-Server nicht.

■ FortiGate SSL-Inspection

Verbindungen zwischen Webapplikationen und Web-Browsern bedienen sich häufig der SSL Verschlüsselung. Dies erhöht die Sicherheit der Datenübertragung, verhindert jedoch, dass die Security Module eine Analyse der eintreffenden Daten vornehmen können. Eine FortiGate Appliance ist in der Lage, eine SSL

Verbindung zu terminieren, die Daten zu entschlüsseln, zu analysieren und anschließend eine gesicherte SSL Verbindung zum Client aufzubauen. So ist gewährleistet, dass sowohl eintreffende als auch ausgehende Daten den Sicherheitsansprüchen des Unternehmens genügen.

■ FortiGate Bandbreiten-Management

Viele Anwendungen wie E-Mail, Video- und Audio-Streaming, Voice over IP, FTP und die zunehmende Nutzung von Webapplikationen in der Cloud lassen den Bandbreitebedarf extrem in die Höhe schnellen. In Spitzenzeiten genügt dann die zur Verfügung stehende Bandbreite nicht mehr, um alle Anwendungen adäquat zu bedienen. Die Folge sind drastische Leistungseinbrüche oder sogar der Abbruch von Verbindungen. Insbesondere bei Sprachübertragung sind jedoch derartige Aussetzer nicht akzeptabel.

Die in FortiOS integrierten Mechanismen bieten vielfältige Optionen Anwendungen zu privatisieren, ihnen Bandbreite zu garantieren oder diese zu limitieren. So kann für einzelne Applikationen Quality of Service (QoS) gewährleistet werden. Insbesondere in Verbindung mit der integrierten Applikationskontrolle und den sog. Identity Based Policies (userspezifische Regelwerke) ist es möglich, die Nutzung von Anwendungen sehr filigran zu kontrollieren.

■ FortiGate Layer 2 und Layer 3 Routing

Jede FortiGate Appliance verfügt über eine leistungsfähige Routing Engine. Damit sind sowohl statische wie auch dynamische Routing Konzepte realisierbar. Mittels dieser Optionen ist z. B. Load Balancing, regelabhängiges Routing, oder Routing im transparenten Modus

möglich. Es werden die gängigen Routingprotokolle wie z.B. RIP, BGP oder OSPF unterstützt. Insbesondere in komplexen VPN Umgebungen ist eine leistungsfähige Routing Engine zwingend erforderlich.

■ FortiGate Netzwerkzugriffskontrolle (NAC)

Die häufigen Veränderungen in Unternehmensnetzwerken – bedingt durch Umzüge, den Wechsel von Endgeräten und die Nutzung von Mobile Devices – machen es erforderlich, dass eine Zugriffskontrolle erfolgt. Dabei wird geprüft, ob auf dem Endgerät definierbare Sicherheits- und andere Anwendungen installiert sind. Zum Beispiel kann festgestellt werden, ob auf dem Endgerät ein FortiClient in seiner aktuellsten Version läuft. Ebenso wird geprüft, ob zwingend erforderliche Anwendungen auf dem Endgerät verfügbar sind.

Endpoints, die diese Prüfung nicht bestehen, werden entweder auf eine Website umgeleitet, wo ggf. die erforderliche Software heruntergeladen werden kann, oder sie werden in Quarantäne gestellt. Via SNMP kann die FortiGate auch mit einem Switch kommunizieren und diesen veranlassen, den zugehörigen Port zu deaktivieren.

■ FortiGate VoIP und SIP Security

Aufgrund der zunehmenden Implementierung von VoIP stehen sowohl Unternehmen als auch Service Provider vor der Herausforderung, Telefoniedienste hochverfügbar und in der gewohnten „analogen“ Qualität bereitstellen zu müssen. Ist es bei vielen Standardanwendungen unproblematisch, wenn deren Antwortzeiten im Millisekunden- oder sogar Sekundenbereich variieren, ist dies bei Sprache völlig inakzeptabel, da dies zu einer deutlich spürbaren Qualitätsminderung (=Unverständlichkeit) führt. Quality of Service (QoS) für VoIP ist damit eine der großen Herausforderungen.

Ein Aspekt von QoS ist aber auch die generelle Verfügbarkeit, welche durch die Nutzung von IP-basierender Infrastruktur den dort seit langem bekannten Sicherheitsbedrohungen ausgesetzt und damit gefährdet ist. Daher ist es wichtig, bereits vorhandene IT-Security-Infrastruktur dahingehend zu prüfen, ob sie sich auch zum Schutz von VoIP-Diensten eignet – und ggf. entsprechende Erweiterungen oder sogar einen Ersatz zu planen.

Ein sicherheitsrelevanter Aspekt bei VoIP-Diensten ist die Tatsache, dass während eines VoIP-Telefonats Ports dynamisch geöffnet und geschlossen werden – dies wird von vielen Standard-Firewalls nicht unterstützt, weshalb für VoIP oft ein großer Port-Bereich standardmäßig geöffnet ist (um diesen Dienst überhaupt nutzen zu können) und somit Angreifern das leichte Eindringen ins Unternehmensnetz ermöglicht.

Die Fortinet VoIP Firewall erkennt anhand des überprüften Datenverkehrs, welche Ports für den Sprachverkehr dynamisch geöffnet werden sollen und wann sie wieder geschlossen werden müssen. Dieser dynamische Prozess unterstützt auch NAT (auf IP, SIP, SDP und RTP). Viele Kunden arbeiten inzwischen mit Fortinets FortiGate Systemen, um Video-, Daten- und Voice-Traffic vor weitverbreiteten Echtzeit-Traffic-Problemen zu schützen, darunter: Session Hijacking, Server-Imitation, Nachrichten-Modifizierungen, Sitzungsabbrüche und Denial-of-Service Angriffen (DoS).

Ein weiterer Vorteil von FortiGate Lösungen für Video-konferenzen ist, dass die bereitgestellte Sicherheit für die Endanwender transparent bleibt. Es besteht keine Notwendigkeit, Änderungen in den Video-Systemen vorzunehmen.

Schutz von Unified Communication und NGN/IMS Netzwerken

Ab FortiOS 4.2. bieten FortiGate Appliances eine Vielzahl von Carrier-grade Schutzmechanismen für SIP-Daten. Einige sind im Folgenden aufgeführt:

Deep SIP Message Inspection analysiert die Header Syntax für SIP und SDP. Bei Erkennung von Syntax-Verletzungen können entsprechende Gegenmaßnahmen konfiguriert werden, u.a. automatische SIP-Antwort-Nachrichten, um den SIP-Server zu entlasten. Die Methodik bietet u.a. Schutz vor weitverbreiteten SIP Fuzzing Angriffen.

SIP Message Rate Begrenzung erlaubt die Begrenzung der Anzahl von SIP Nachrichten pro SIP Request Methodik. So können DoS-Angriffe auf SIP-Server verhindert werden.

RTP Pin-Holing leitet nur solche RTP/RTCP Pakete weiter, die mit der individuellen Session Beschreibung des zugeordneten SIP-Dialogs konform sind. Nach Beendigung eines SIP-Dialogs schließt die FortiGate die sog. Pin-Hole automatisch. RTP/RTCP Pin-Holing wird

von FortiASICs unterstützt, so dass eine größtmögliche Durchsatzrate bei äußerst geringem Jitter erzielt wird.

Stateful SIP Dialog Tracking FortiOS analysiert SIP Nachrichten und schützt so vor ungewollten oder unerlaubten SIP Paketen, die nicht dem zugeordneten SIP-Dialog entsprechen. So ist es z. B. möglich, schadhafte SIP BYE-Nachrichten zu erkennen und zu blockieren, die nicht in den Kontext des entsprechenden SIP Dialogs passen.

■ FortiGate IPv6 Security

Seit der Vergabe der letzten IPv4-Adresse in 2010 gewinnt IPv6 zunehmend an Bedeutung auch in kleineren Unternehmen. Haben Carrier und einige größere Unternehmen bereits eine vollständige oder partielle Umstellung durchgeführt, wird durch die Einführung neuer Services, die künftig nur noch via IPv6-Adressierung erreichbar sein werden, der Druck hinsichtlich einer Migration von IPv4 nach IPv6 zunehmend ansteigen.

IPv6 bietet viele Features, die über Jahre bei IPv4 vermisst wurden: Limitierung bei der Anzahl der verfügbaren Adressen, faire Verteilung von Adressen, integrierte Quality of Service (QoS) Funktionen, bessere Multimedia-Unterstützung und verbessertes Handling von fragmentierten Daten. IPv6 verfügt über 128-Bit-Adressen (IPv4: 32-Bit) und eliminiert dadurch voraussichtlich die Notwendigkeit von NAT, da pro Person weltweit ca. 1 Milliarde IP-Adressen zur Verfügung stehen.

IPv4 und IPv6 – gemischte Welten

Durch die sich über mehrere Jahre erstreckende Umstellungsphase werden IT-Infrastruktur-Komponenten über lange Sicht beide Welten – also IPv4 und IPv6 – unterstützen müssen. Dies stellt viele der vorhandenen Komponenten, insbesondere Routing- und Security-Instanzen, vor große Herausforderungen.

Bei der Umstellung und Migration auf IPv6 stellt sich daher die Frage zum richtigen Umgang mit Malware. IPv6 bietet Malware Autoren mehr Möglichkeiten, ihren Schadcode stärker zu verbreiten, als mit IPv4. Ein trivialer Grund sind die IPv6 Stacks, mit denen es wenig Praxiserfahrung gibt. Den IPv4 Stacks liegen

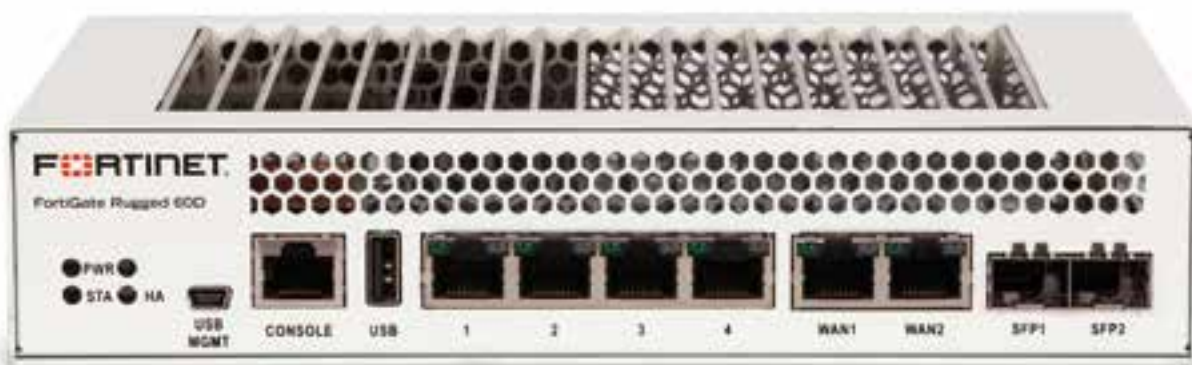
Dekaden an Erfahrung zugrunde, und trotzdem finden sich in diesen immer noch diverse Schwachstellen. IPv6 Stacks in Betriebssystemen oder in Programmen gehen weitgehend jungfräulich in den harten Internet-Alltag. Bereits heute gibt es schon über hundert bekannte Schwachstellen in diversen IPv6 Protokollstacks und Implementierungen.

IPv6 Malware

Fast alle IPv4-basierten Exploits sind auch IPv6 fähig. Das bedeutet, dass Virenschreiber im ersten Schritt nichts oder nur wenig anpassen müssen, damit ein Exploit auch IPv6 fähig ist. Sie können jedoch zusätzliche Mechanismen von IPv6 nutzen, um sich noch stärker, noch unbemerkter und damit effizienter zu verbreiten.

Ähnliches gilt für einen Wurm. „I Love You“ nutzt Email zur Weiterverteilung, hier ist keine Anpassung notwendig. Wohingegen „Conficker“ sich selbsttätig über eine Schwachstelle in Windows über IPv4 verbreitet, aber über eine Anpassung auch IPv6 tauglich gemacht werden kann.

Hackertools für IPv6 sind bereits seit Jahren im Umlauf. IPv6 Tunneldienste bergen ein hohes Risiko unbemerkt Daten an bestehenden Sicherheitslösungen vorbei zu schleusen. Malware kann zum Beispiel unbemerkt IPv6 auf einem Host aktivieren, einen IPv6 Tunneldienst starten und diesen Pfad nach außen öffnen. Ein klassisches Beispiel ist hier Teredo. Damit ließe sich nicht einfach nur IPv6 durch eine bestehende IPv4 NAT Firewall tunneln, sondern die IPv6 Adresse dieses Hosts wäre auch grundsätzlich von außen erreichbar.



IPv6 Security

Es wird offensichtlich, dass klassische, IPv4-basierte Schutzmechanismen in IPv6 oder gemischten Umgebungen keinen ausreichenden Schutz mehr bieten können. Ebenfalls liegt auf der Hand, dass ein reines „IPv6-ready“-Zertifikat genau in Augenschein genommen werden muss: Nicht jede einzelne Security-Instanz in einer UTM- oder NGFW-Appliance ist automatisch damit erfasst; vielmehr gilt es, die einzelnen Module auf ihre IPv6-Fähigkeit zu prüfen.

Durch seine jahrelange enge Kooperation mit Carriern und Service Providern, die im Bereich IPv6 zu den sog. „Early Adoptern“ gehören und deren Infrastruktur bereits in großen Teilen IPv6-fähig ist, hat Fortinet umfangreiche Erfahrungen in diesem Segment sammeln können. Darauf ist es auch zurückzuführen, dass FortiGate Lösungen bereits heute eine Vielzahl von IPv6-Security-Features bieten und bedenkenlos in eine zu migrierende Umgebung integriert werden können – bzw. eine Migration bei bereits vorhandenen FortiGate Appliances in puncto Security problemlos ist.

FortiGate Ruggedized – die Lösung für Industrie und Produktions-Umgebungen

Industrielle Kontrollsysteme werden mit immer mehr gezielten Angriffen konfrontiert und sind besonders anfällig für Angriffe mit dem Potential, weitläufige Ausfälle zu verursachen. Traditionelle Sicherheitssysteme sind für Büro-Umfelder gedacht. Das FortiGateRugged-60D ist eine auf die Industrie spezialisierte, komplette Sicherheitslösung, die speziellen Schutz für essentielle Industrienetzwerke gegen schädliche Angriffe bietet.

Ruggedized Protection for Harsh Environments
FortiGateRugged-60D erfüllt die Leistungsziele und Zuverlässigkeitsstandards für den Betrieb im anspruchsvollen Umfeld der Schaltstation. Es wurde für den zuverlässigen Einsatz unter schweren elektrischen und umweltlichen Bedingungen entwickelt, einschließlich großer Elektro- oder Funkinterferenzen und vieler Temperaturbereiche.

Industrial Network Security FortiOS bietet auf der Ruggedized-Plattform spezifischen Schutz für industrielle Netzwerke unter Einsatz von Sicherheitstechnologien wie Antivirus & IPS, während der Update-Dienst und das Team von Bedrohungsexperten von FortiGuard Echtzeitschutz bieten, um die neusten Angriffe ohne Intervention des Administrators zu identifizieren.

EIGENSCHAFTEN AUF EINEN BLICK

Network Services and Support

Built-in DHCP, NTP, DNS Server and DNS proxy (available on most models)
 FortiGuard NTP, DDNS and DNS service
 Interface modes: sniffer, port aggregated, loopback, VLANs (802.1Q and Trunking), virtual hardware, software and VLAN switches (available on most models)
 Static and policy routing
 Hybrid WAN support: load balancing and redundancy with link health check on monitoring using TWAMP
 Support USB 3G/4G Wireless WAN modems
 Dynamic routing protocols:
 - RIPv1 and v2, OSPF v2 and v3, ISIS, BGP4
 Multicast traffic: sparse and dense mode, PIM support
 Content routing: WCCP and ICAP
 Traffic shaping and QoS per policy or applications: shared policy shaping, per-IP shaping, maximum & guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS) and Differentiated Services (DiffServ) support
 IPv6 Support: Management over IPv6, IPv6 routing protocols, IPv6 tunnelling, firewall and UTM for IPv6 traffic, NAT46, NAT64, IPv6 IPSEC VPN

WAN Optimization, Web Cache and Explicit Proxy^

Inline and out-of-path WAN optimization topology, peer to peer and remote client support
 Transparent Mode option: keeps the original source address of the packets, so servers appear to receive traffic directly from clients.
 WAN optimization techniques: protocol optimization and byte caching
 WAN Optimization protocols supported: CIFS, FTP, HTTP(S), MAPI, TCP
 Secure Tunneling option: use AES-128bit-CBC SSL to encrypt the traffic in the WAN optimization tunnel.
 Tunnel sharing option: multiple WAN optimization sessions share the same tunnel.
 Web caching: object caching that accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency. Supports caching of HTTP 1.0 and HTTP 1.1 web sites.
 SSL Offloading with Web caching:
 - Full mode: performs both decryption and encryption of the HTTPS traffic.
 - Half mode: only performs one encryption or decryption action.
 Option to exempt certain web sites from web caching with URL patterns.
 Support advanced web caching configurations and options:
 - Always revalidate, Max cache object size, negative response duration, fresh factor, Max/Min/Default TTL, proxy FQDN, Max HTTP request/message length, ignore options, cache expired objects, revalidated prama-no-cache
 Explicit web & FTP proxy: FTP, HTTP, and HTTPS proxying on one or more interfaces
 Proxy auto-config (PAC): provide automatic proxy configurations for explicit web proxy users.
 Proxy chaining: web proxy forwarding to redirect web proxy sessions to other proxy servers.
 Web proxy forwarding server monitoring and health checking
 IP reflect capability
 Load balancing for forward proxy and proxy chaining
 Explicit web proxy authentication: IP-Based authentication and per session authentication
 WAN optimization and web cache monitor

User & Device Identity Control

Local user database & remote user authentication service support: LDAP, Radius and TACACS+, 2-factor authentication
 Single-sign-on: Windows AD, Novell eDirectory, FortiClient, Citrix and Terminal Server Agent, Radius (accounting message), POP3/POP3S, user access (802.1x, captive portal) authentication
 PKI and certificates: X.509 certificates, SCEP support, Certificate Signing Request (CSR) creation, auto-renewal of certificates before expiry, OCSP support
 Device Identification: device and OS fingerprinting, automatic classification, inventory management
 User and device-based policies

Integrated Token Server

integrated token server that provisions and manages physical, SMS and Soft One Time Password (OTP) Tokens

Firewall

Operating modes: NAT/route and transparent (bridge)
 Schedules: one-time, recurring
 Session helpers & ALGs: dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 O, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)
 VoIP traffic support: SIP/H.323 /SCCP NAT traversal, RTP pin holing
 Protocol type support: SCTP, TCP, UDP, ICMP, IP
 Section or global policy management view
 Policy objects: predefined, customs, object grouping, tagging and coloring
 Address objects: subnet, IP, IP range, GeoIP (Geography), FQDN
 NAT configuration: per policy based and central NAT Table
 NAT support: NAT64, NAT46, static NAT, dynamic NAT, PAT, Full Cone NAT, STUN

VPN

IPSEC VPN:
 - Remote peer support: IPSEC-compliant dialup clients, peers with static IP/dynamic DNS
 - Authentication method: certificate, pre-shared key
 - IPSEC Phase 1 mode: aggressive and main (ID protection) mode
 - Peer acceptance options: any ID, specific ID, ID in dialup user group
 - supports IKEv1, IKEv2 (RFC 4306)
 - IKE mode configuration support (as server or client), DHCP over IPSEC
 - Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128, AES192, AES256
 - Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
 - Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14
 - XAuth support as client or server mode
 - XAuth for dialup users: Server type option (PAP, CHAP, Auto), NAT Traversal option
 - Configurable IKE encryption key expiry, NAT traversal keepalive frequency
 - Dead peer detection
 - Replay detection
 - Autokey keep-alive for Phase 2 SA
 IPSEC Configuration Wizard for termination with popular 3rd party devices
 IPSEC VPN deployment modes: gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, VPN termination in transparent mode,
 IPSEC VPN Configuration options: route-based or policy-based
 Customizable SSL VPN portal: color themes, layout, bookmarks, connection tools, client download
 SSL VPN realm support: allows multiple custom SSL VPN logins associated with user groups (URL paths, design)
 Single-sign-on bookmarks: reuse previous login or predefined credentials to access resources
 Personal bookmarks management: allow administrators to view and maintain remote client bookmarks
 SSL portal concurrent users limiting
 One time login per user options: prevents concurrent logins using same username
 SSL VPN web mode: for thin remote clients equipped with a web browser only and support web application such as:
 - HTTP/HTTPS Proxy, FTP, Telnet, SMB/CIFS, SSH, VNC, RDP, Citrix
 SSL VPN tunnel mode: for remote computers that run a variety of client and server applications, SSL VPN client supports MAC OSX, Linux, Windows Vista and with 64-bit Windows operating systems
 SSL VPN port forwarding mode: uses a Java Applet that listens on local ports on the user's computer. When it receives data from a client application, the port forward module encrypts and sends the data to the SSL VPN device, which then forwards the traffic to the application server.
 Host integrity checking and OS check (for windows terminals only) prior to SSL tunnel mode connections
 MAC host check per portal
 Cache cleaning option just before the SSL VPN session ends
 Virtual desktop option to isolates the SSL VPN session from the client computer's desktop environment
 VPN monitoring: view and manage current IPSEC and SSL VPN connections in details
 Other VPN support: L2TP client (on selected models) and server mode, L2TP over IPSEC, PPTP, GRE over IPSEC

FEATURE SUMMARY

SSL Inspection

Inspect SSL Encrypted traffic option for IPS, application control, antivirus, web filtering and DLP

IPS

IPS engine: 7,000+ up-to-date signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic pull or push signature update, threat encyclopedia integration

IPS Actions: default, monitor, block, reset, or quarantine (attackers IP, attackers IP and Victim IP, incoming interface) with expiry time

Filter Based Selection: severity, target, OS, application and/or protocol

Packet logging option

IP(s) exemption from specified IPS signatures

IPv4 and IPv6 Rate based DOS protection (Available on most Models) with threshold settings against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/CMP session flooding (source/destination)

IDS sniffer mode

Active bypass with bypass Interfaces (selected models) and FortiBridge

Application Control

Detects over 3,000 applications in 18 Categories:

Botnet, Collaboration, Email, File Sharing, Game, General Interest, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others)

Custom application signature support

Supports detection for traffic using SPDY protocol

Deep Application visibility: login names, files/video activities and information

Filter based selection: by category, popularity, technology, risk, vendor and/or protocol

Actions: block, reset session, monitor only, application control traffic shaping

SSH Inspection

Anti-Malware / Advanced Threat Protection

Botnet server IP blocking with global IP reputation database

Antivirus database type selection (on selected models)

Flow-based Antivirus: protocols supported - HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, ICQ, YM, NNTP

Proxy-based Antivirus:

- Protocol Support: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, ICQ, YM, NNTP

- External cloud-based file analysis (OS sandbox) support

- File submission blacklisting and whitelisting

- File quarantine (local storage required)

- Heuristic scanning option

Web Filtering

Web filtering inspection mode support: proxy-based, flow-based and DNS

Manually defined web filtering based on URL, web content & MIME header

Dynamic web filtering with cloud-based realtime categorization database: over 250 Million URLs rated into 78 categories, in 70 languages

Safe Search enforcement: transparently inserts Safe Search parameter to queries.

Supports Google, Yahoo!, Bing & Yandex, definable YouTube Education Filter

Additional features offered by proxy-based web filtering:

- Filter Java Applet, ActiveX and/or cookie

- Block HTTP Post

- Log search keywords

- Rate images by URL

- Block HTTP redirects by rating

- Exempt scanning encrypted connections on certain categories for privacy

- Web Browsing quota by categories

Web filtering local categories & category rating override

Web filtering profile override: allows administrator to temporarily assign different profiles to user/user group/IP

Restrict access to Google Corporate Accounts only

Proxy avoidance prevention: proxy site category blocking, rate URLs by domain & IP address, block redirects from cache & translation sites, proxy avoidance application blocking (application control), proxy behavior blocking (IPS)

Data Leak Prevention (DLP)

Web filtering inspection mode support: proxy-based, flow-based and DNS

DLP message filter:

- Protocol supported: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP

- Actions: log only, block, quarantine user/IP/interface

- Predefined filter: credit card number, Social Security ID

DLP File Filter:

- Protocol Supported: HTTP-POST, HTTP=GET,SMTP, POP3, IMAP, MAPI, FTP, NNTP

- Filter options: size, file type, watermark, content, if encrypted

DLP watermarking: allows filter files that pass through the FortiGate unit and contain a corporate identifier (a text string) and a sensitivity level (Critical, Private, and Warning) hidden in a watermark. Support Windows and Linux free watermarking tools.

DLP fingerprinting: generates a checksum fingerprint from intercepted files and compare it to those in the fingerprint database.

DLP archiving: records full content in email, FTP, IM, NNTP, and web traffic

Endpoint Control

Manages network devices via client software:

- Posture checking: enforce client software installation and desired settings

- Client configuration provisioning: push and update client configurations such as VPN and web filtering settings accordingly to device type/group and/or user/usergroup

- "Off-net" security enforcement: detects when not protected by security gateway, activates provisioning security settings

- allows client activities logging implementation

Client software support: Windows, OS X, iOS, Android

Vulnerability Scanning

Network Vulnerability Scan: protect network assets (servers and workstations) by scanning them for security weaknesses.

- On-demand or scheduled

- Scan Modes: Quick, standard or Full

- authenticated scanning

Vulnerability Result: detailed scan results are logged with direct reference on threat encyclopedia

Wireless and Switch Controller

Manages and provisions settings for local and remote Thin Access points or switches (selected models)

Set up access and authentication methods for SSIDs and VLANs, supports integrated or external captive portal, 802.1x, preshared keys

WiFi Security: Rogue AP suppression, wireless IDS

Wireless topology support: Fast roaming, AP load balancing, Wireless Mesh and bridging

High Availability

High availability modes: active-passive, active-active, virtual clusters, VRRP, FG-5000 series clustering

Redundant heartbeat interfaces

HA reserved management interface

Failover:

- Port, local & remote link monitoring

- stateful failover

- subsecond failover

- Failure detection notification

Deployment Options:

- HA with link aggregation

- Full mesh HA

- Geographically dispersed HA

Standalone session synchronization

Administration, Monitoring & Diagnostics

Management Access: HTTPS via web browser, SSH, telnet, console

Web UI administration language support: English, Spanish, French, Portuguese, Japanese, Simplified Chinese, Traditional Chinese, Korean

Central management support: FortiManager, FortiCloud hosted service, web service APIs

Systems Integration: SNMP, sFlow, Netflow, syslog, alliance partnerships

Rapid deployment: Install wizards, USB auto-install, local and remote script execution

Dynamic, real-time dashboard status & drill-in monitoring widgets

■ FortiManager

Zentralisiertes Management

FortiManager Appliances stellen eine Vielzahl von notwendigen und hilfreichen Tools zur Verfügung, mit denen eine Fortinet-basierende Sicherheits-Infrastruktur optimal und effektiv administriert und kontrolliert werden kann. So sind die Verwaltung, das RollOut, Updates oder die zentrale Konfiguration von bis zu vielen tausend Fortinet-Appliances und FortiClients einfach, übersichtlich und kostengünstig realisierbar.

FortiManager Appliances reduzieren drastisch Verwaltungskosten und vereinfachen Prozesse. Die Erkennung von Geräten, das Gruppen-Management, Auditing-Möglichkeiten sowie umfangreiche Funktionen, mittels derer komplexe VPN-Umgebungen verwaltet werden können, sind nur einige wenige der zahlreichen Features dieser Appliance-Serie. In Verbindung mit den FortiAnalyzer Lösungen für Logging und Reporting stehen äußerst leistungsfähige zentrale Management-Instanzen für jede Unternehmensgröße zur Verfügung.

Mandantenfähigkeit

Da die FortiManager Appliance-Serie auf bis zu mehrere tausend Geräte und Clients skaliert, stehen integrierte mandantenfähige Management-Domänen zur Verfügung. Diese sog. ADOMs (Administrative Domains) bieten maximale Flexibilität bei der Verwaltung von unternehmensinternen Abteilungen, unabhängigen Unternehmensbereichen oder für das Management vieler tausend verschiedener Kunden. Durch zusätzliche und optionale globale ADOMs sind weitere zentrale Administration-Features verfügbar die gleichermaßen für große Unternehmen wie für Service Provider hochinteressant sind.

Hierarchische Objektdatenbank

Die Erstellung von Templates zur Gerätekonfiguration ermöglichen das schnelle Einbinden und Konfigurieren einer Fortinet-Appliance. Jede DOM verfügt über eine gemeinsame Objektdatenbank, auf die alle Geräte und Policies zugreifen können. So sind identische oder ähnliche Konfigurationen innerhalb einer Gruppe sehr einfach zu erstellen. Mittels der optionalen Global Policy Add-Ons können übergreifende Regelwerke und globale Daten-

banken, die für alle FortiOS im System zur Verfügung stehen, erstellt werden.

Lokales Security Content Hosting

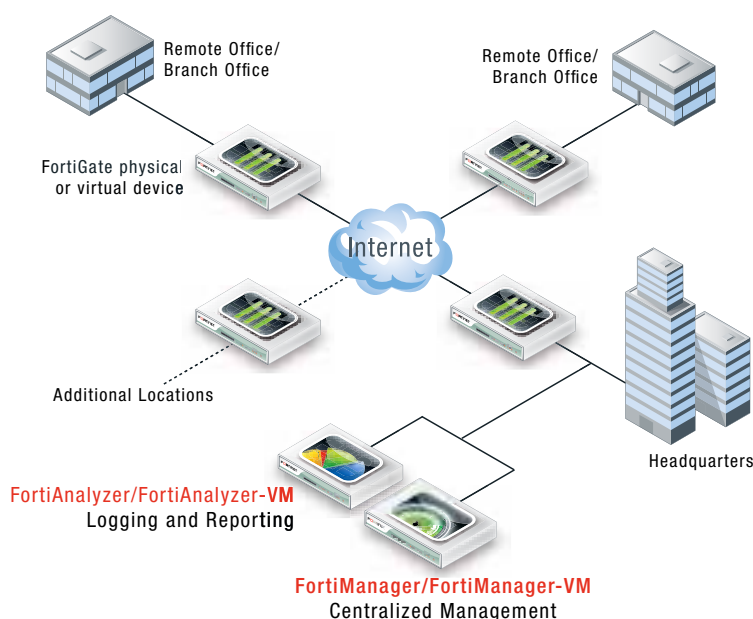
Die Option, Security Updates lokal bereitzustellen, bietet Administratoren bessere Kontrollmöglichkeiten über Updates und reduziert und verbessert Antwortzeiten für Rating Datenbanken. So können Antivirus-, Intrusion Prevention-, Schwachstellenmanagement-, Web Filtering- und Anti-Spam-Updates lokal zur Verfügung gestellt werden.

Vereinheitlichtes Managementmodell

Ein optimierter und einheitlicher Work-Flow ermöglicht die einfache Konfiguration mehrerer verschiedener Management-Komponenten via ADOM. Dazu stehen Objekte und dynamische Objekte, Import- und VPN-Wizards, VDOM-Synchronisation, Geräte-Übersichten und GUI-basierende Skripte zur Verfügung.

FortiManager XML API

Die FortiManager XML-API ist eine Web-Service-Schnittstelle, die der Automatisierung von Managementprozessen dient. Kunden einer privaten oder öffentlichen Cloud können so z.B. in ein Provisioning-System integriert werden. Außerdem können FortiGate Systeme über ein Web-Service-Interface konfiguriert werden.



■ FortiAnalyzer

Zentralisiertes Reporting

Die FortiAnalyzer Produktfamilie bietet Echtzeit-Netzwerk-, Logging-, Analyse- und Reporting-Funktionen in Form einer Appliance, die auf sichere Weise Log-Daten von Fortinet-Geräten und auch von Produkten anderer Hersteller zusammenführen. Sämtliche Informationen über Traffic, Events, Viren, Angriffe, Web-Inhalte und EMail-Daten können archiviert und ausgewertet werden. Zusätzlich können geographisch und chronologisch verteilte Securitydaten zentral gesammelt, korreliert und analysiert werden.

Umfangreiches Reporting

Eine umfassende Auswahl an Standardberichten gehört ebenso zum Lieferumfang, wie die Möglichkeit, beliebige benutzerdefinierte Reports zu generieren. FortiAnalyzer bietet außerdem erweiterte Sicherheitsmanagement-Funktionen wie die Archivierung von Quarantäne-Dateien, Ereignis-Korrelation, Vulnerability Assessments, Traffic-Analyse und die Archivierung von E-Mail-, Webzugriffs-, Instant-Messaging- und Dateitransfer-Inhalten.

Auf diese Weise können sich Unternehmen jeder Größenordnung einen einfachen und konsolidierten Überblick über ihre Security-Situation verschaffen. Durch eine Vielzahl von voreingestellten und kunden-spezifischen Reports werden Unternehmen ebenfalls bei ihren Compliance-Bestrebungen unterstützt.

Schwachstellenmanagement

Die FortiAnalyzer Systeme bieten sehr umfangreiche Scan-Möglichkeiten, die es erlauben, sämtliche Endgeräte in einem Netzwerk zu erkennen und zu priorisieren, Schwachstellen zu katalogisieren, Ports zu erstellen und Listen mit Handlungsempfehlungen auszugeben. Unternehmen, die PCI DSS Compliance nachweisen müssen, können auf voreingestellte Schwachstellen-Scans und -Reports zurückgreifen.

Wesentliche Funktionen:

- **UTM- & Trafficberichte**
Analysieren Sie regelmäßig Ihr Sicherheitsprofil und Ihre Traffic-/Bandweitenmuster mit einem neuen gemeinsamen UTM-/Trafficbericht.

- **Integrierte Berichtsvorlagen**

Nutzen Sie die anpassbaren PDF-Vorlagen für bunte, umfassende und grafische Netzwerksicherheits- und Nutzungsberichte.

- **Import/Export von Vorlagen**

Exportieren Sie nach dem Erstellen eines Berichts die Konfiguration auf einen anderen FortiAnalyzer oder ADOM und bearbeiten Sie sie.

- **Ereignisverwaltung**

Überwachen Sie wichtige Ereignisse mit einmaligen Analysemöglichkeiten für potentiell anomales Verhalten, um sie dem IT-Administrator vorzulegen.

- **Drill-Downs**

Grafische Echtzeitdarstellungen der Traffic-, Web-, E-Mail- und Bedrohungsaktivitäten.

JSON- und XML-(Internetdienste) APIs

- APIs sind für alle FortiAnalyzer Hardwaremodelle und virtuellen Geräte verfügbar.
- JSON-API – Ermöglicht MSSPs/großen Firmen FortiAnalyzer Berichte, Diagramme, Datensätze und Objekte zu manipulieren.
- XML API – Ermöglicht IT-Administratoren, FortiAnalyzer schnell zu konfigurieren und Berichte zu erstellen.
- Zugang zu Tools, Beispielcodes, Dokumentation und Interaktion mit der Fortinet-Entwickler-Community durch Beitritt zum Fortinet Developer Network (FNDN).

Log Viewer

- Anzeige von vergangenen oder Echtzeit-Protokollen
- Auswahl aus Traffic, Ereignis oder UTM-Protokollen
- Suche nach Gerät, ADOM oder im Ganzen
- Protokollfilter und Suchmöglichkeiten
- Gezielte Untersuchung mit Protokolldetails
- Intuitive Icons für Länder, Anwendungen, etc.

DLP-Archivierung

- Untersuchung von DLP-Content-Archiven
- Unterstützte Archivtypen u. A.: E-Mail, HTTP, FTP, IM
- Archivtext anzeigen oder Dateien herunterladen

Alarmierung

- Umfassende Alarmeinstellung
- Auslösung nach Schwere, bestimmten Ereignissen, Aktionen und Zielen
- Festlegung verschiedener Schwellen für die Anzahl von Ereignissen in einem bestimmten Zeitraum
- Anzeige und Suche vergangener Alarme
- Benachrichtigung per E-Mail/SNMP oder Erstellung eines Syslog-Ereignisses

Von FortiAnalyzer unterstützte Systeme

- FortiGate Sicherheitssysteme für Mehrfachbedrohungen
- FortiMail Nachrichtensicherheitssysteme
- FortiClient Endpunktssicherheitssuite
- FortiWeb Webanwendungssicherheit
- FortiManager zentralisiertes Management
- Jedes Syslog-kompatible System

FortiCloud

Mit FortiCloud stellt Fortinet einen gehosteten Security-Management- und Log-Analyse-Service zur Verfügung, der FortiGate und FortiWifi Appliances unterstützt. FortiCloud bietet zentrales Reporting, Traffic-Analyse, Konfigurations-Management sowie Log-Speicherung ohne die Notwendigkeit zusätzlicher Hard- und Software.

Durch einfaches Hinzufügen über einen kostenlosen Account können FortiGate Appliances auf diese Weise einfach administriert und ausgewertet werden. Bei einem größeren Speicherbedarf als 1GB pro Appliance kann der jeweilige Geräte-Account individuell und kostengünstig um weitere Kapazität (200GB) ergänzt werden. Gespeichert werden können Traffic-Verlauf, System Events sowie Web-, Applikations- und Security-Events.

FortiCloud Bestandteile

- **Dashboard** – System- und Log-Widgets inkl. Echtzeit-Monitor
- **Log Viewer** – Echtzeit Log-Übersicht mit Filtern auf alle kritischen Vorkommnisse oder unklare Ereignisse
- **Drilldown Analysis** – User- und Netzwerk-Aktivitäts-Analysen zur granularen Visualisierung aller Aktionen
- **Report Generator** – Erstellung von kundenspezifischen oder vorkonfigurierten Reports in verschiedenen Formaten (inkl. PDF), um z. B. Compliance nachzuweisen oder bestimmte Netzwerk-Verhaltensweisen zu dokumentieren.
- **Device Management** – Management von Software Updates und Standardisierung über das gesamte Netzwerk



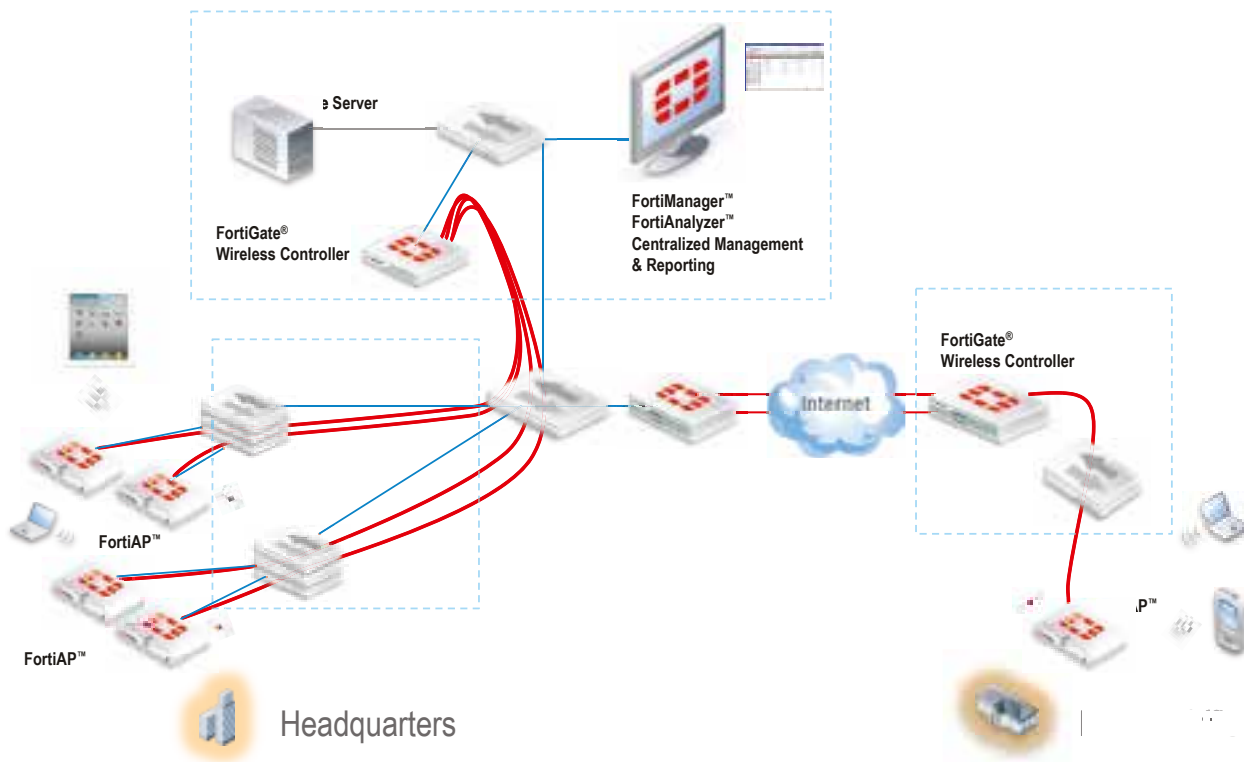
■ FortiAP – Sichere WLAN Infrastruktur mit den Access Points FortiAP

Fortinet ist bekannt für Sicherheitslösungen, die umfassenden und höchsten Schutz sowohl für kabelgebundene wie kabellose (Wireless) Netzwerke bieten. Die neue Serie von Thin Access Points in Verbindung mit einer Vielzahl von Wireless Controllern in jeder FortiGate Appliance bietet High-Performance Netzwerkzugänge mit integrierter Content-Security. Durch die Kombination eines Wireless Controllers mit einer FortiGate Plattform (größer als Modell FG30B) wird das Sicherheitsniveau des kabelgebundenen LANs automatisch auf die WLAN-Umgebung übertragen.

Der gesamte WLAN-Traffic wird so identitätsbasiert über die UTM-Engines der FortiGate Appliance geleitet und dort entsprechend analysiert, und es werden nur autorisierte Verbindungen zugelassen. Durch diese Integration ist es möglich, von einer einzigen Konsole aus den Netzwerkzugang zu überwachen, Regelwerke einfach und schnell upzudaten und den Datenverkehr und die Einhaltung von Compliance-Regeln kontinuierlich zu prüfen.

Da jede FortiGate Appliance (größer als Modell FG30B) ab FortiOS 4.1. über diese Wireless-Controller Funktionalität verfügt, können bereits bestehende Gateways durch ein einfaches Betriebssystem-Update um dieses Feature erweitert werden – die Anschaffung einer zusätzlichen Plattform mit einer eigenen Administrations-Oberfläche entfällt. Durch die hohe Performance und große Reichweite der neuen FortiAP Serie ist der Aufbau einer hochsicheren und leistungsstarken WLAN-Infrastruktur einfach und kostengünstig möglich.

In vielen Anwendungsszenarien erübrigt sich unter Umständen sogar das Installieren einer Verkabelung bis zum Arbeitsplatz, da die Durchsatzraten der WLAN-Lösung vielfach äquivalent hoch sind. Die Thin WLAN Access Point Serie FortiAP umfasst Modelle für jeden Anwendungsbereich, sowohl Indoor als auch Outdoor.



Voucher-Erstellung für Gastzugänge

Mittels einer integrierten sog. Receptionist-GUI können auf einfache Weise Vouchers für den WLAN-Zugang erstellt und ausgedruckt werden. Die Zugänge können z.B. zeitlich beschränkt werden, gleichzeitig für eine Gruppe von Personen erstellt und komfortabel verwaltet werden.

Remote Access Points und Local Break Out

Mobile Mitarbeiter, Teleworker sowie Niederlassungen eines Unternehmens benötigen ebenfalls WLAN. Dieses muss denselben Sicherheitsanforderungen der

Zentrale genügen und auch von dieser managebar sein. Mittels der FortiGate und FortiAP Integration ist beides möglich. Überdies kann Traffic auch über einen sog. Local Break Out in der jeweiligen Niederlassung verbleiben und muss nicht zwingend – je nach Regelwerk – über die Zentrale geroutet werden.

Remote Access Points stellen darüberhinaus eine elegante, kleine und kostengünstige Möglichkeit dar, kleine Home-Offices oder mobile Mitarbeiter sehr schnell und einfach an die Zentrale anzubinden und über eine CAPWAP-Verbindung eine verschlüsselte Verbindung dorthin zu etablieren.

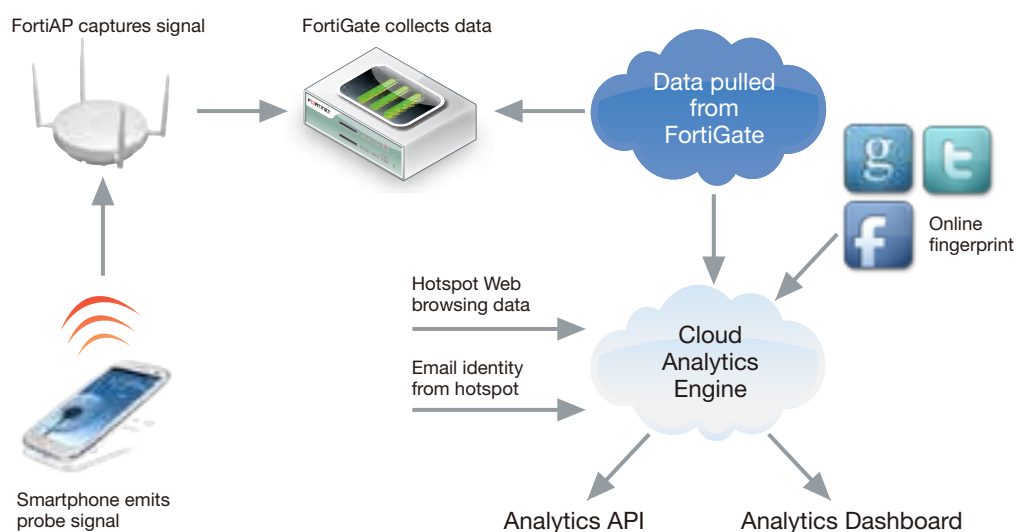
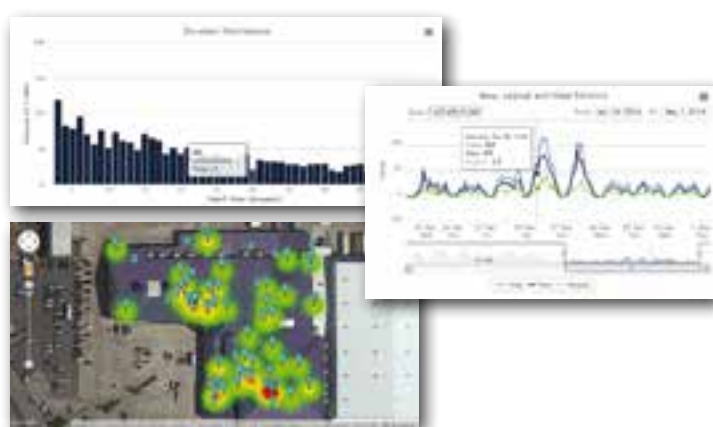


■ FortiPresence

Onlinehändler ziehen zunehmend Vorteile aus der Vielfalt von Informationen, die sie über das Verhalten ihrer Kunden sammeln können. Fortinet's Presence Analytics Lösungen bieten derartigen Unternehmen einen detaillierten Einblick in das Verhalten ihrer Kunden und damit die Möglichkeit, deren Kaufverhalten zu beeinflussen und damit die Kundenbindung zu steigern.

Durch die zunehmende Nutzung von Smartphones und der starken Expansion von Onlinehändlern wie Amazon stehen klassische Einzelhändler vor einem immer wiederkehrenden Problem: Kunden testen und betrachten ein Produkt im Verkaufsraum, um es dann online zu bestellen. Durch die über Jahre gesammelten Informationen über Kunden haben Onlinehändler einen gravierenden und zugleich unfairen Vorteil gegenüber klassischen Einzelhändlern.

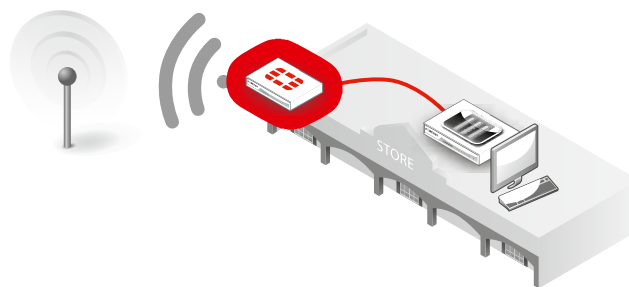
FortiPresence bietet in Verbindung mit Fortinet's WLAN-Lösungen die Möglichkeit, das Verhalten von Kunden auch für Einzelhändler zugänglich zu machen. Da Smartphones regelmäßig nach Accesspoints scannen, können über diese Signale deren Aufenthaltsort sowie deren Bewegungen registriert und entsprechend ausgewertet werden. So ist es möglich, Kunden während des Verweilens vor einem Schaufenster auf einem Monitor bereits die richtigen Produkte in Echtzeit zu präsentieren, um sie dann beim Betreten des Geschäfts gezielt anbieten und vorführen zu können. Dies ist jedoch nur eine von vielen Möglichkeiten, die auf diese Weise gesammelten Informationen auszuwerten und zu nutzen.



■ FortiExtender 3G/4G WAN Extender

Die Abhängigkeit von einer funktionierenden WAN-Verbindung in einer zunehmend digitalisierten Welt nimmt deutlich zu – und wird in immer kürzeren Abständen immer wichtiger. Downtime ist nicht nur unerwünscht, sondern kann in vielen Fällen zu großem Schaden führen. Insbesondere bei verteilten Umgebungen wie z. B. großen Filial-Strukturen ist der Ausfall der WAN-Verbindung zu vermeiden, könnten so z.B. Kassensysteme oder Niederlassungen ohne Local Break Out nicht mehr sinnvoll arbeiten.

Der FortiExtender 3G/4G schafft hier Abhilfe, indem er für eine existierende FortiGate Security-Plattform ein Back-up zur primären WAN-Verbindung bietet. Das Betriebssystem einer FortiGate initiiert in einem Fehlerfall einen nahtlosen Übergang von der drahtgebundenen zur drahtlosen Kommunikation des FortiExtenders. Durch die inzwischen sehr hohen Übertragungsraten



von 3G- und 4G-Verbindungen findet der FortiExtender ebenfalls Anwendung als primäre WAN-Verbindung in verteilten Umgebungen.

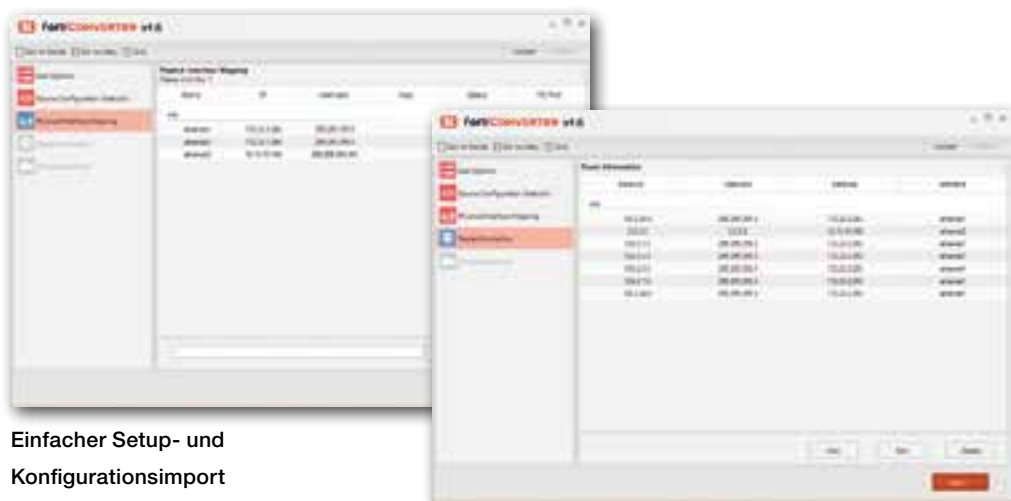
FortiExtender sind echte Plug-and-Play-Geräte. Sobald sie an eine FortiGate angeschlossen werden, erscheinen sie als normales Netzwerkinterface in FortiOS. FortiExtender sind sowohl als Indoor- als auch als Outdoor-Modelle verfügbar.

■ FortiConverter

Eine der größten Herausforderungen und oft sogar ein „Show-Stopper“ ist die Migration einer existierenden Security-/Firewall-Installation in eine neue, Next Generation-Architektur. Eine Vielzahl von Regeln, deren Sinn und Zweck nicht selten undokumentiert ist, muss überarbeitet und in ein neues, strukturiertes und damit oft auch wesentlich performanteres Regelwerk überführt werden. Dabei geht es gerade in größeren Umgebungen nicht selten um mehrere tausend Regeln und Objekte, die an eine neue Lösung angepasst werden müssen – ein oft teures und langwieriges Unterfangen.

Mit FortiConverter kann dieser Prozess drastisch vereinfacht und verkürzt werden. Der MultiVendor-Support für

Cisco, Juniper, CheckPoint und Sonicwall bietet auch für heterogene Umgebungen eine ideale Basis. Durch einen hohen Grad an Automatisierung sind nur geringfügige Änderungen und Anpassungen erforderlich. Ebenso werden über die Jahre entstandene Fehler eines Regelwerks erkannt und können beseitigt werden.



Einfacher Setup- und Konfigurationsimport

Physischer Abbau einer bestehenden Architektur

■ FortiToken

Einmal-Passwort für starke Authentifizierung

Mit dem FortiToken 200 können Unternehmen leistungsfähige aber dennoch preiswerte und einfache starke 2-Faktor-Authentifizierung einführen. Dabei handelt es sich um Einmal-Passwort-Token (auch One-Time-Passwort/OTP), mit dem Unternehmenszugänge gesichert werden können, die bisher auf schwache 1-Faktor-Authentifizierung (z.B. statische Passwörter) ausgelegt sind.

Mit dem FortiToken können Administratoren sowohl mobile als auch unternehmensinterne Anwender in ein erweitertes Sicherheitskonzept einbeziehen. Dabei ist das FortiToken Teil der umfangreichen Produktstrategie zur Multi-Faktor-Authentifizierung, mit der sichergestellt wird, dass nur noch autorisierte Personen Zugang zu unternehmenskritischen Daten erhalten.

Nutzen der vorhandenen Fortinet-Appliances

Jede FortiGate Appliance bietet ab FortiOS 4.3. die Möglichkeit der 2-Faktor-Authentifizierung. Ein externer und nicht selten kostenintensiver Server sowie kostspielige Token mit Jahreslizenzen können so entfallen. Die zeitbasierenden FortiToken bieten starke Authentifizierung für IPsec VPN, SSL VPN, WLAN Captive Portals und FortiGate Administrator Login. Dabei ist das Token ständig mit der FortiGate zeitsynchronisiert.

FortiGuard Schlüsselmanagement

Das FortiGuard Center sorgt für ein sicheres und komfortables Schlüsselmanagement. Nach Registrierung der Token-S/N an der FortiGate verteilt das FortiGuard Security Center die zugehörigen Schlüssel über eine Cloud-basierende sichere Infrastruktur an die jeweiligen FortiGates. Wenn es eine identitätsbasierende Regel erfordert, ist eine FortiGate so in der Lage, das 6-stellige Token-Passwort gegen seine eigene Datenbank zu verifizieren.

Integration mit FortiAuthenticator

In Verbindung mit dem FortiAuthenticator kann die Nutzung des FortiTokens sehr einfach auf komplexere FortiGate Umgebungen sowie auf 3rd-Party-Systeme erweitert werden. Nähere Informationen finden sich im separaten Kapitel zum FortiAuthenticator in dieser Broschüre.

Standards und AAA Server Kompatibilität

Das FortiToken ist kompatibel mit herkömmlichen lokalen und Remote-Access-Servern inklusive Active Directory, LDAP und RADIUS. Die FortiGate verwaltet somit gleichzeitig sowohl die Backend-Kommunikation mit diesen Servern als auch die 2-Faktor-Authentifizierung mit dem Anwender. In Kombination mit einer FortiGate entspricht das FortiToken dem OATH Standard.

Widerstandsfähiges Design

Das FortiToken wird in einem manipulationssicheren Gehäuse ausgeliefert und der veränderungsresistente interne Speicher verhindert Manipulationen am dynamischen Passwort-Generator.



FortiToken 200CD

Mit FortiToken 200CD, bei dem die Token-Seeds auf den Servern der FortiGuard Labs sicher hinterlegt sind, bietet Fortinet eine Option, die Kunden diese Seeds auf einer verschlüsselten CD bereitstellt. Somit hat der Anwender die Möglichkeit, diese Token-Keys in eigener Verantwortung sicher zu verwahren und die Mehrfachnutzung (ein Token auf mehreren FortiGates) wird stark vereinfacht.

FortiToken 300 – USB-SmartCard Token

Für besonders sichere Umgebungen bietet sich das FortiToken 300, eine USB-SmartCard-Token für PKI-Infrastrukturen an. Es bietet OneTime-Passwords und Verschlüsselung über einen Hardware-Chip in Verbindung mit einer Client-Software. Letztere ist für Windows, Linux und MacOS verfügbar. Es werden Microsoft CAPI und PKCS#11 APIs unterstützt. Die Lizenz ist – wie auch bei den übrigen FortinetToken Lösungen, eine Einmal-Lizenz, so dass keine weiteren Kosten entstehen.



FortiToken Mobile

Ergänzend zu den Hardware-Token ist es mit dem FortiToken Mobile möglich, iOS und Android-Geräte als Token zu nutzen. Diese OATH-kompatible Lösung bietet ein zeitbasiertes OneTime-Password-Verfahren und entbindet den User von der Nutzung eines zusätzlichen Geräts (HW-Token). Durch ein dynamisches Generieren der Token-Seeds sowie dessen verschlüsselte Übertragung und Speicherung ist dieses Verfahren deutlich sicherer als vergleichbare Methoden.

Das FortiToken Mobile ist mit den FortiGate Appliances ebenso nutzbar wie mit der Authentifizierungs-Lösung FortiAuthenticator und somit universell einsetzbar. Es basiert auf einer Einmal-Lizenz, die eine wiederholte Lizenzierung überflüssig macht und somit Kosten spart. Jede FortiGate Appliance ab FOS5 bietet die kostenlose Nutzung von zwei FortiToken Mobile beispielsweise für Admin-Accounts.



■ FortiAuthenticator – Zentraler AAA-Server

Der FortiAuthenticator dient als zentrale Instanz für das User Identity Management. Es werden 2-Faktor-Authentifizierung, Identitäts-Verifikation und Netzwerkzugriffskontrolle (NAC) unterstützt.

Durch den Support von LDAP und RADIUS und die Integration des Fortinet Single Sign On Features der FortiGate Serie in Active Directory stehen umfangreiche Funktionen zur Zugriffskontrolle der Anwender zur Verfügung. FortiAuthenticator ermöglicht die zentrale Zugriffssteuerung auf FortiGate und 3rd-Party-Systeme, VPN-Zugänge und Webseiten.

Zwei Faktor Authentifizierung

Der FortiAuthenticator erweitert die 2-Faktor-Authentifizierung mittels Token auf Umgebungen mit vielen verteilten FortiGate Appliance und 3rd-Party-Lösungen, die RADIUS oder LDAP-Authentifizierung unterstützen.

Die im FortiAuthenticator gespeicherten Informationen zur Benutzeridentität in Verbindung mit den Authentifizierungs- Informationen des FortiToken stellen sicher, dass nur autorisierte Anwender Zugang zu sensiblen Unternehmensdaten erlangen. Neben zusätzlicher Sicherheit unterstützt diese Vorgehensweise Unternehmen bei der Einhaltung von Compliance-Vorgaben oder anderen Regularien.

Vereinfachtes Management und Benutzerfreundlichkeit

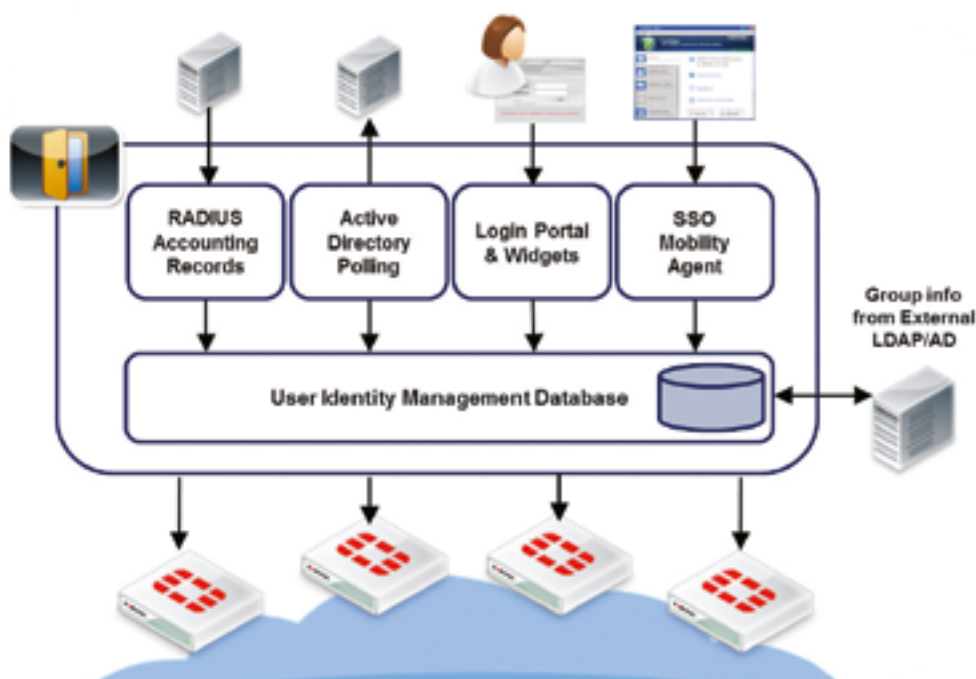
Durch die Bereitstellung sämtlicher erforderlicher Dienste sowie die Speicherung aller Benutzerdaten auf einem einzigen System, werden die Kosten für sichere Nutzer-Authentifizierung deutlich gesenkt.

Der FortiAuthenticator ist in wenigen Minuten betriebsbereit und wurde speziell zur Vereinfachung von Authentifizierungs-Prozessen entwickelt. Dies schließt die Integration in bereits vorhandene Authentifizierungs-Datenbanken ebenso ein, wie die reibungslose Token-Initialisierung.

Eine weitere Arbeitserleichterung bietet das Self-Service-Portal, über welches Anwender ihre Zugangsdaten anfordern können, wenn sie ihr Token verloren oder vergessen haben.

Fortinet Single Sign On (FSSO)

Fortinet Single Sign On (FSSO) steigert die Benutzerfreundlichkeit, indem es die Anzahl der erforderlichen LogIns deutlich reduziert. Die Integration von FSSO in Active Directory ermöglicht die Konfiguration und Nutzung von identitätsbasierten Regelwerken, um Netzwerk- und Datenzugriff in Abhängigkeit von Gruppenzugehörigkeiten festzulegen.



■ FortiClient Endpoint Security

Personal Computer (PCs), Desktops und Laptops ermöglichen den Anwendern den Zugang zu Unternehmensapplikationen und vertraulichen Daten – vom internen Netzwerk ebenso wie von unterwegs. Während sich die Produktivität verbessert, erhöht der Zugriff von außen gleichzeitig das Sicherheitsrisiko für die interne Netzwerkinfrastruktur. Die Rechner sind sogenannten „Blended Threats“ ausgesetzt, also Angriffen, die sich gleichzeitig verschiedener Mechanismen bedienen, wie z. B. Viren, Trojaner, Würmer, Spyware, Keylogger, Botnetzen, Spam und Internet-Attacken.

Während Netzwerk-Sicherheitsarchitekturen verschiedene Segmente voneinander isolieren, können sich PCs, die sich innerhalb eines Subnetzes befinden, durchaus gegenseitig infizieren. Anwender verstoßen oft unabsichtlich gegen die Sicherheitsrichtlinien, in dem sie tragbare Speichermedien (USB Sticks, MP3-Player, Kameras, mobile Festplatten) einsetzen, nicht darauf achten, ob ihr Virenschutz auf dem aktuellen Stand ist oder sogar die Personal Firewall ausschalten.

Anwender, die auf Webseiten mit unangemessenen oder schädlichen Inhalten zugreifen, gefährden die Integrität des Netzwerks, beeinflussen die Produktivität negativ, verursachen Sicherheitsrisiken und lösen unter Umständen rechtliche Auseinandersetzungen aus.

Während Sicherheitstechnologien, wie z. B. AntiVirus Software, einen bestimmten Angriffspunkt schützen und somit nur für bestimmte Angriffsarten zur Verfügung stehen, versagen diese Methoden bei „Blended Threats“ und sind auch nicht in der Lage, Zugangsrichtlinien umzusetzen.

FortiClient Security Suite

Der neue FortiClient in seiner aktuellen Version 5 konsolidiert die bisher verfügbaren Varianten und erweitert seinen Einsatzbereich auf zusätzliche Plattformen, darunter auch die gängigsten mobilen Betriebssysteme iOS und Android. Dadurch – und durch eine Vielzahl weiterer Funktionen – ist sein Einsatz auch in heterogenen und BYOD-(Bring Your Own Device) Umgebungen möglich.

Seine einzeln aktivierbaren Sicherheits-Engines reichen von einer leistungsstarken AntiVirus-Einheit über WebFilter bis hin zu VPN-Clients und Schwachstellen-Management-Funktionen. In Verbindung mit einer FortiGate kann der FortiClient zentral administriert und überwacht werden; ebenfalls ist auf diese Weise ein lokales Logging und Auswerten der Client-Daten möglich.

Einfachste und kostengünstige Lizenzierung

In der Standalone-Version ist der FortiClient – inkl. aller Updates – kostenlos unter www.forticlient.com zum Download verfügbar. Diese Option ermöglicht es kleinen Unternehmen und auch Privatpersonen, ihre Endgeräte effektiv zu sichern und überdies kostengünstige VPN-Verbindungen zu einer zentralen FortiGate bereitzustellen.

Größere Unternehmen mit den Anforderungen, ihre Endgeräte zentral zu administrieren, zu updaten und zu überwachen, können mithilfe einer FortiGate Appliance die FortiClients zentral verwalten. Auf diese Weise können unterschiedliche Profile erstellt und ausgerollt werden, auch in Abhängigkeit von der aktuellen Netzwerk-Verbindung („on-net/off-net“).

Ebenso können die Logdaten der Clients zentral gesammelt und ausgewertet werden. Pro FortiGate Appliance sind 10 FortiClients kostenfrei integrier- und managebar. Bei weiteren Clients ist der Erwerb einer permanenten Einmallizenz erforderlich.

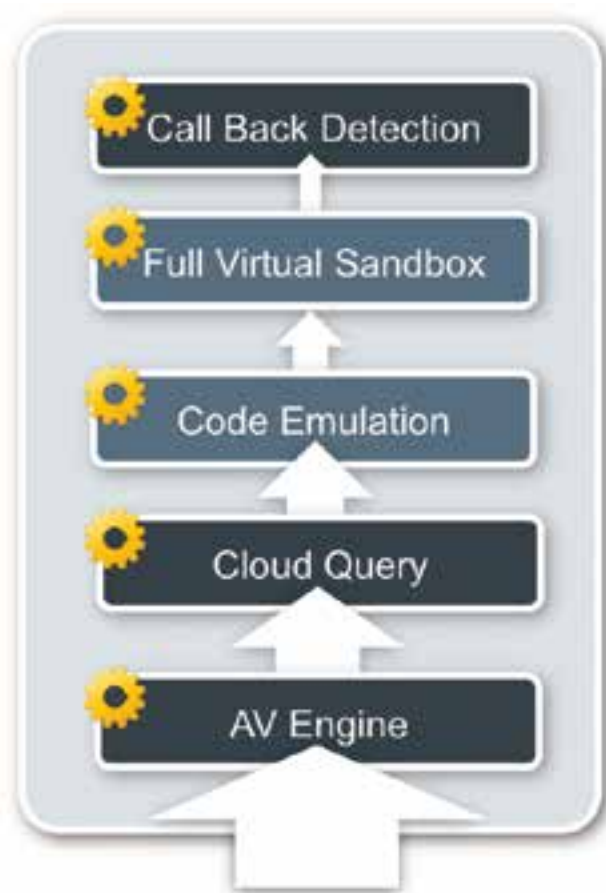
■ FortiSandbox

Mithilfe der leistungsstarken Sicherheits-Appliance (die auch als VM-Lösung verfügbar ist) FortiSandbox können Unternehmen und Behörden hochgefährliche Angriffe wie zum Beispiel Advanced Persistent Threats (APTs) zuverlässiger erkennen und verhindern. APTs sind zielgerichtete und besonders effektive Cyber-Attacken auf IT-Infrastrukturen und vertrauliche Daten, die zumeist über einen längeren Zeitraum ausgeführt werden.

Das neue Fortinet-Angebot verbindet eine einzigartige Dual-Level-Sandbox mit der dynamischen Aufdeckung von Bedrohungen, Echtzeit-Dashboard sowie umfassenden Reporting-Funktionen in einer einzigen Anwendung, die sich sowohl in vorhandene Netzwerke als auch mit Fortinets FortiGate Next Generation Firewalls (NGFW) sowie den FortiMail E-Mail-Gateway-Appliances integrieren lässt.

Die NGFWs von Fortinet agieren als erste Verteidigungslinie – sie erkennen und minimieren Sicherheitsbedrohungen. In Kombination mit der FortiSandbox sind die Appliances in der Lage, besonders verdächtige oder risikoträchtige Dateien mit neuartigen Erkennungsmethoden zu identifizieren und zu untersuchen. Aufgrund der Ergebnisse dieser Analyse werden dann alle Schutzmechanismen – basierend auf dem gesamten Lebenszyklus der erkannten Bedrohung – aktualisiert.

Mit der neuen FortiMail Version 5.1 können Fortinet E-Mail-Gateways sowohl verdächtige als auch High-Risk-Dateien in E-Mails identifizieren und sie zur weiteren Untersuchung an die FortiSandbox weiterleiten.



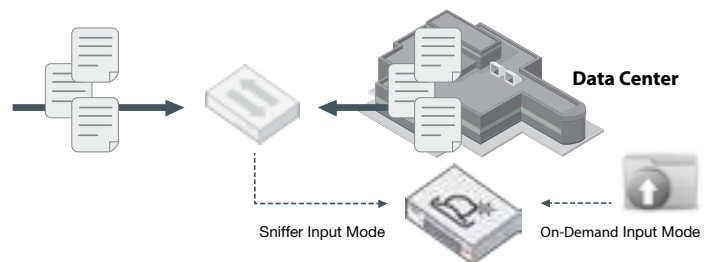
Mehrstufige Arbeitsweise einer FortiSandbox

Die FortiSandbox auf einen Blick

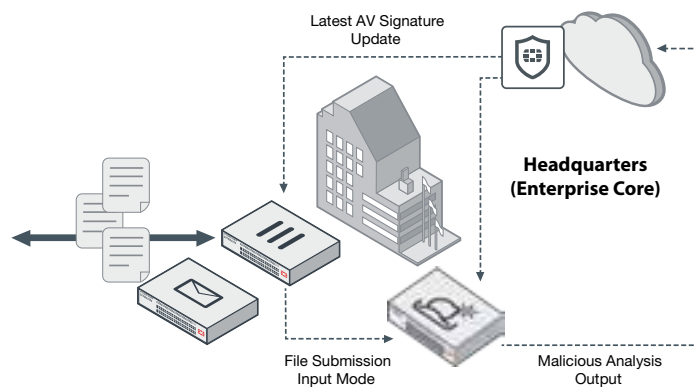
Die FortiSandbox lässt sich standalone in vorhandene Netzwerke integrieren, ohne weitere Konfigurationen vornehmen zu müssen. Alternativ ermöglicht die Lösung eine Ergänzung von Fortinets FortiGate und FortiMail Plattformen, um deren Erkennungsmechanismen weiter zu verbessern.

Getreu der Fortinet-Philosophie konsolidiert die FortiSandbox hochentwickelte Threat Detection- und Intelligence-Dienste über viele Protokolle und Funktionen hinweg in einer einzigen besonders leistungsstarken und kostengünstigen Appliance. Deren Herzstück ist eine Dual-Level Sandbox, die neuartige und komplexe Angriffsmethoden auf virtuelle Maschinen (VM) ebenso aufdeckt wie die Vielzahl immer raffinierterer Cyber-Attacken.

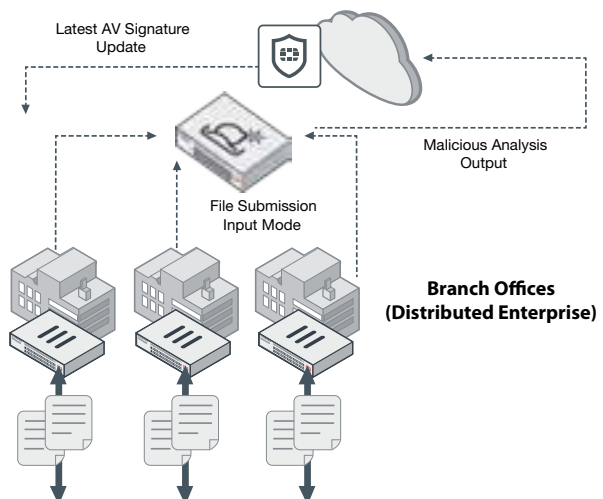
Betriebsmodus „Standalone“



Betriebsmodus „FortiGate/FortiMail Integrated“



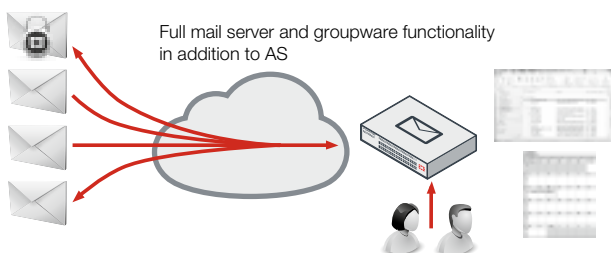
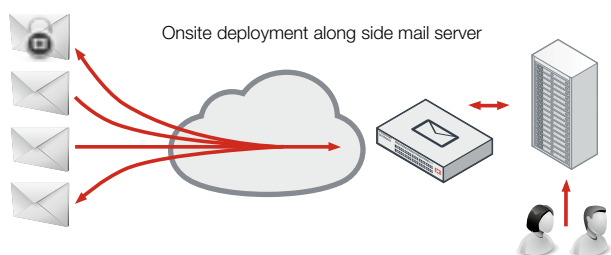
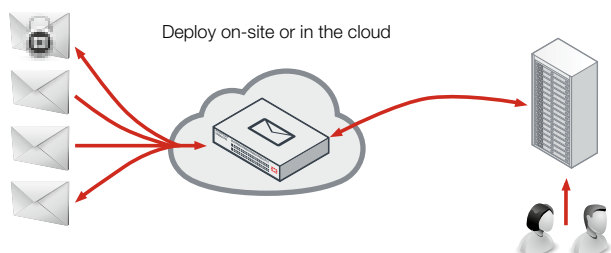
Betriebsmodus „Distributed FortiGate Integrated“



FortiMail

Email-Security

FortiMail Appliances und virtuelle Appliances bieten leistungsfähigen und umfangreichen Schutz für E-Mail-Dienste in Unternehmen jeder Größenordnung – von KMU über Carrier, Service Provider bis hin zu sehr großen Enterprise-Unternehmen. Fortinets jahrelange Erfahrung im Schutz von Netzwerken gegen Spam, Malware und andere message-basierende Angriffe spiegelt sich auch in dieser Lösung wider.



Sicherer Schutz von Mail-Systemen

FortiMail schützt E-Mail-Systeme davor, selbst zum Malware-Verteiler zu werden. Durch ihre bidirektionale Architektur schützen FortiMail Systeme Netzwerke vor eingehenden Spam-Nachrichten und Malware, bevor diese im Unternehmen Schaden anrichten können. Gleichzeitig wird verhindert, dass schadhafte ausgehende E-Mails von anderen externen Gateways zu einem Blacklisting des Unternehmens führen. Insbesondere letztere Eigenschaft ist für Service Provider essenziell und höchst geschäftskritisch. FortiMail

Appliances bieten High-Performance E-Mail Routing und Security durch die Verwendung von mehreren höchst genauen Anti-Spam-Filtern. In Verbindung mit Fortinets marktführenden Antivirus-&-Anti-Spyware-Modulen wird höchste Sicherheit garantiert.

Verschiedene Betriebsmodi

Verschiedene Anwendungsszenarien ermöglichen zusätzliche Flexibilität beim Einsatz der Appliance. Diese kann sowohl im Gateway Modus, im Transparent Modus sowie im Server Modus betrieben werden.

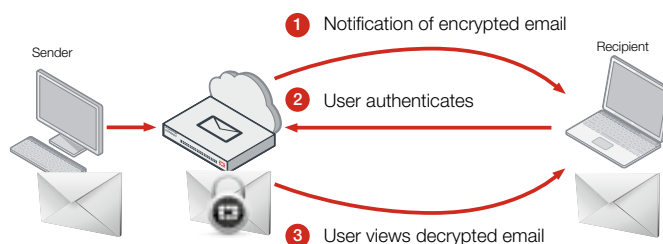
Einfaches Lizenzmodell

Das User-unabhängige Lizenzmodell garantiert niedrige Anschaffungs- und Betriebskosten und ermöglicht so eine transparente Planung.

FortiMail Identity based Encryption (nutzerabhängige Mail-Verschlüsselung)

Eine neue Funktionalität wertet die erfolgreiche und leistungsfähige Mail-Security-Appliance FortiMail noch weiter auf. Seit dem Release 4.2 der FortiMail Familie können abhängig von Nutzer (Sender) oder Mailinhalten (Wörterbücher) Mails verschlüsselt versendet werden. Dabei ist es nicht notwendig, dass auf Seiten des Senders oder des Empfänger zusätzliche Client-Software installiert wird.

Unternehmen können also kostenlos und ohne weiteren Administrationsaufwand sensible E-Mail-Kommunikation verschlüsseln und damit deutlich sicherer übertragen. Durch die sog. Identity Based Encryption werden Mails abhängig von Nutzergruppe, Nutzer oder spezifischen in der Mail enthaltenen Wörtern verschlüsselt.



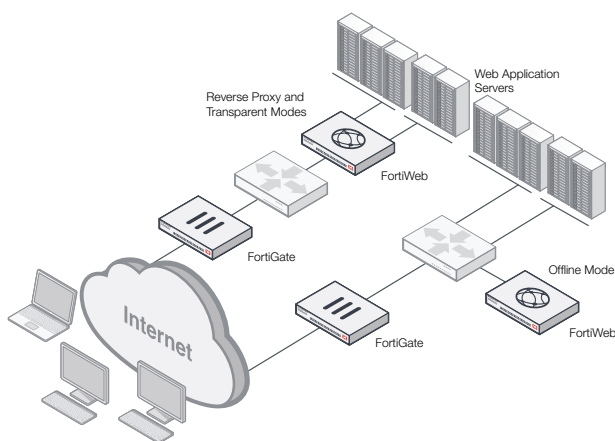
■ FortiWeb Web Application Firewall

Web-Anwendungen und Sicherheit

Web-Anwendungen nutzt nahezu jeder wie selbstverständlich – und es ist ebenso selbstverständlich, dass sie auch funktionieren. War in der Vergangenheit oft nur die Rede von E-Mail-Portalen, CRM-Portalen und ähnlichem – also reinen Business-Anwendungen für Mitarbeiter – so haben wir es inzwischen im Alltag eines jeden Internetnutzers damit zu tun. Sogenannte Provisioning-Portale werden für alle Lebensbereiche selbstverständlich.

Das Programmieren von Web-Anwendungen ist in der Regel fokussiert auf eine bestimmte Funktionalität und auf eine möglichst schnelle Verfügbarkeit, sowie geringe Kosten. Das Einbinden der notwendigen Sicherheits- Algorithmen erfordert einen mit zunehmender Komplexität der Anwendung immens steigenden Programmieraufwand – und erzeugt damit Kosten sowie eine Verzögerung der Auslieferung. Gleiches gilt für die ständigen Updates der Anwendung, die nur noch selten statisch und unverändert bleibt.

Security in eine Web-Applikation einzubinden stellt somit nicht nur eine große Herausforderung dar – es wird in den meisten Fällen schlicht vernachlässigt oder nur oberflächlich umgesetzt.



Die verschiedenen Betriebsmodi der FortiWeb

Web Services und „normale“ Firewalls

Eine normale Firewall – auch wenn sie über IPS und Applikationskontrolle verfügt – ist nicht in der Lage, Web FortiWeb Web-Application-Servers FortiWeb Service-basierte Angriffe zu erkennen und abzuwehren.

Web Services – also die den Web-Applikationen zugrundeliegenden Funktionen (die oft von mehreren Anwendungen gleichzeitig genutzt werden) – bedienen sich einer eigenen Beschreibungssprache (WSDL) und eines eigenen Protokolls (SOAP). Sowohl WSDL als auch SOAP beinhalten keinerlei Security-Mechanismen, beschreiben bzw. übertragen aber alle Parameter eines Web-Dienstes transparent.

Es liegt auf der Hand, dass Angriffe in Form von z.B. Manipulationen des Services sehr leicht möglich sind. Ein Beispiel hierfür sind sog. XDoS-Angriffe, die auf nur einem einzigen System mit wenigen Byte Code erzeugt werden können, da XML rekursive Strukturen erlaubt. Mit einem simplen Eingriff ist so z.B. eine Endlosschleife „programmierbar“, die denselben Effekt erzeugt, wie ein „normaler“ DoS Angriff, für den i.d.R. mehrere tausend Systeme manipuliert und fremdgesteuert werden müssten.

Sicherheit mit FortiWeb

Die FortiWeb Produktfamilie repräsentiert eine solche integrierte Web-Security Appliance-Serie. Mit unterschiedlichen Leistungsdaten aber einheitlichem Feature-Set adressiert sie Unternehmen aller Größenordnungen, Application Service Provider (ASPs) und SaaS-Anbieter.

FortiWeb stellt neben den Modulen Web Application Firewall, XML Firewall und Web Traffic Optimizer auch ein Applikations-basiertes Load Balancing sowie einen leistungsfähigen Schwachstellenscanner bereit.

Mit der Möglichkeit des Auto-Learning ist es überdies möglich, den Traffic zu Web Anwendungen regelmäßig zu analysieren und entsprechende Security Profile automatisiert zu erstellen – ohne Eingriff in die vorhandene Netzwerkinfrastruktur oder die zu schützende Applikation.

Ein Policy Wizard sowie voreingestellte Regelwerke erleichtern den Einsatz und die Inbetriebnahme der FortiWeb Appliances ebenso wie die verschiedenen Anwendungsszenarien als Transparent Inspection, Reverse oder True Transparent Proxy, sowie Offline.

FortiDB Datenbank-Sicherheit

Den erhöhten Schutzbedarf im Datenbankbereich deckt Fortinet mit einer neuen Reihe von Security-Appliances ab, die speziell für das Vulnerability-Assessment in Datenbanken konzipiert ist. Die FortiDB ist eine automatisierte und zentralisierte Sicherheitslösung, die Datenbankapplikationen stabilisiert, indem sie potenzielle Angriffspunkte – etwa Schwachstellen in Passwörtern, Zugriffsberechtigungen und Konfigurationen – aufdeckt. Dabei setzt die Appliance Warnungen an den Systemadministrator ab und bietet Korrekturhilfen an.

Die FortiDB Produktfamilie schützt vor externem und internem Diebstahl von firmeneigenen und persönlichen Daten und erkennt auch Zugriffe scheinbar legitimer Nutzer. Allen Produkten gemeinsam sind die drei Feature-Sets 24x7-Überwachung der Datenbankaktivität, Datenbank-Audits und Vulnerability Assessment. Letzteres sorgt für zusätzliche Sicherheit von Datenbanken, indem Schwachstellen in Passwörtern, Zugangsberechtigungen, fehlende Sicherheits-Updates und falsche oder mangelhafte Konfigurationseinstellungen aufgedeckt werden.



Profilierungsaktivitäten – FortiDB erstellt automatisch Grundlinien für Benutzeraktivitäten bei einfachen Konfigurationsregeln



Dashboard – Das FortiDB Dashboard zeigt wesentliche Schwachstellen und Datenbankaktivitäten Überwachung/Audit Information



Alarmübersicht – Gesamtübersicht über Alarme und Trends



Alarmanalysen – Detaillierte Trendanalysen ermöglichen es den Benutzern, ihre interne Kontrollstruktur zu verbessern.

■ FortiDDoS

Abwehr von DDoS-Angriffen
bis auf Applikationsebene

DDoS – keine „kleine“ Störung, sondern eine ernste Bedrohung

„Hacktivismus“ per Botnets und via Netzwerk-Test-Anwendungen haben im vergangenen Jahr drastisch zugenommen und führten zu einem starken Anstieg sowohl der Anzahl von Angriffen als auch DDoS-Angriffen auf Applikationsebene. Diese Angriffe legen ganze Webseiten lahm, indem sie die Anwendungs-Server und/oder die Internetverbindung überlasten.

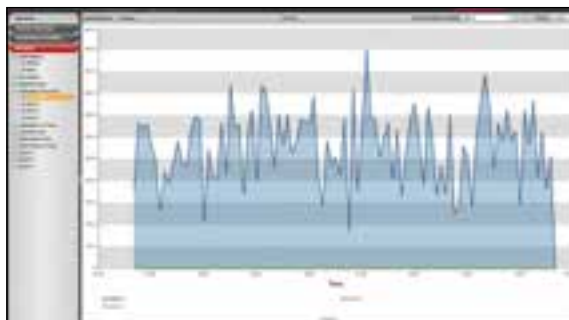
Da Unternehmen immer häufiger Software-as-a-Service (SaaS)-Angebote und andere Public-Cloud basierte Dienste verwenden, werden DDoS-Attacken zu einem sehr ernsthaften Problem für CIOs und CSOs – und dies bereits bei der Entscheidung, ob sie Dienste überhaupt in die Cloud auslagern oder ihre Systeme und Daten weiterhin inhouse betreiben und verwalten möchten.

Die häufigsten Beweggründe für DDoS-Attacken sind heute entweder finanziell oder politisch geprägt. Finanziell motivierte Angreifer versuchen, Websitebetreiber zu erpressen, indem sie einen ersten Angriff starten und Zahlungen verlangen, die dann zukünftige Angriffe vermeiden sollen. Politisch motivierte Angreifer hingegen reagieren auf eine Aktivität des Unternehmens und stören oder unterbrechen in der Regel wichtige Geschäftsprozesse.

Motivunabhängig wirken sich Ausfallzeiten nicht nur auf die Kunden, Partner und Angestellten des Unternehmens aus, sondern können auch seine Marke und Glaubwürdigkeit stark schädigen.

FortiDDoS Appliances schützen effektiv

Die FortiDDoS Appliances wurden zum Erkennen und Abwehren von intelligenten DDoS-Attacken entwickelt und bieten somit optimalen Schutz für das Netzwerk. Die Appliances verfügen über anwendungsspezifische Chipsets (sog. ASICs), die auch hochentwickelte und hochvolumige DDoS-Angriffe blockieren und trotzdem extrem niedrige Latenz (weniger als 26 µs) garantieren.



So ist die Verfügbarkeit von kritischen Systemen, Servern und Anwendungen auch bei DDoS-Angriffen mit hoher Frequenz gewährleistet. Neben einer detaillierten Einsicht in den Netzwerkverkehr in Echtzeit sowie automatischem Schutz gegen gezielte DDoS-Attacken bieten die FortiDDoS Appliances als einzige Lösungen Netzwerk-Virtualisierung und ein automatisches und kontinuierliches Traffic-Baselining. Die Virtualisierungsfunktion verhindert, dass Angriffe auf ein einzelnes Segment des Netzes Auswirkungen auf andere Bereiche haben.

Dies ist insbesondere für die permanente Verfügbarkeit von Systemen und Applikationen in virtualisierten Umgebungen von Rechenzentren und bei Cloud-Service-Providern von Bedeutung. Das automatische Traffic-Baselining ermöglicht darüber hinaus die Erstellung

eines Netzwerk-Verhaltensmodells, das sich fortlaufend und ohne Eingreifen des Anwenders aktualisiert und damit den Verwaltungsaufwand deutlich reduziert.

FortiDDoS Highlights

Alle FortiDDoS Appliances bieten acht virtualisierte Netzwerkpartitionen mit unabhängigen Schutz-Profilen für virtualisierte Umgebungen, eine automatische Netzwerkverkehrsanalyse und kontextbezogene Richtlinien für Schwellwerte, um maximale Leistungsfähigkeit zu

ermöglichen. Zusätzlich verfügen sie über eine Echtzeit- und eine historische Traffic-Analyse, die außergewöhnlich detaillierte Einblicke in die Top-Attacks, Top-Quellen und Top-Angreifer gewährleistet. Die FortiDDoS Produktreihe bedient sich eines neuartigen Designs für die Beseitigung typischer Leistungsengpässe, indem sichergestellt wird, dass weder CPU noch Betriebssystem Datenpakete verlangsamen.

■ FortiDNS

Schutz von DNS-Servern

DNS-Sicherheit – ein MUSS

Domain Name System (DNS), die Methodik, um Domänen-Namen in IP-Adressen von Geräten (z. B. Servern) zu übersetzen, wird oft als „Lebenselixier“ des Internet bezeichnet. Ohne DNS könnten keine E-Mails versendet werden, würden keine Webseiten gefunden und jeglicher Internetzugang wäre unmöglich. Im Falle der Kompromittierung eines DNS-Systems wären Unternehmen angreifbar und User-Zugriffe auf Webseiten könnten leicht auf schädliche Inhalte umgeleitet werden.

DNS ist eines der kritischsten, aber häufig am wenigsten beachteten Elemente, die kontinuierliche Geschäftsprozesse gewährleisten. Das Problem mit DNS ist seine Komplexität, die Anfälligkeit für Fehlkonfiguration und die Notwendigkeit, es via Command Line Interface zu bedienen.

FortiDNS wurde von Grund auf dahingehend entwickelt, als hoch-sicheres DNS Caching System herkömmliche Lösungen zu ersetzen. Durch seine zu 100 % grafische Benutzeroberfläche werden Konfigurationsfehler nahezu ausgeschlossen.

Sicherheit im Fokus

Wie auch bei anderen Fortinet Lösungen, wird Sicherheit bei FortiDNS großgeschrieben.

Um dies zu erreichen, ist Fortinet eine Technologie-Partnerschaft mit Nominum, einem der führenden Anbieter von DNS-Lösungen, eingegangen. Entwickelt von Fortinet und „Powered by Nominum“ steht für signifikante Verbesserung der Sicherheit im DNS-Umfeld.



■ FortiADC

Application Level Load Balancing

Die Parameter Verfügbarkeit, Performance und Reaktionszeit von (Web-)Anwendungen haben nicht nur zunehmend starken Einfluss auf die Akzeptanz der Nutzer, sondern bestimmen immer häufiger auch den wirtschaftlichen Erfolg von ganzen Unternehmensbereichen. Geschäftskritische Anwendungen wie Portale, Shops, CRM- oder ERP-Systeme usw. müssen daher gut und schnell funktionieren, um ihrem Zweck gerecht werden zu können.

Häufig werden aber die eingangs genannten Parameter durch schlechte Programmierung der Web-Inhalte, falsch dimensionierte und somit überlastete (Web-) Server, oder unflexible Leitungsnutzung negativ beeinflusst. Abhilfe schaffen hier sogenannte Application Load-Balancing-Systeme, die die Last intelligent auf die verfügbaren Server verteilen, Web-Inhalte optimieren

und lokal oder sogar dezentral zwischenspeichern und weitere optimierende Funktionen übernehmen können.

Die neue Serie der FortiADC optimiert die Verfügbarkeit, das Anwendungsverhalten, die Performance sowie die Skalierbarkeit von sowohl mobilen und Cloud- als auch von Enterprise-Anwendungen. Das Design dieser Produktlinie wurde auf eine schnelle, intelligente und sichere Beschleunigung von bandbreitenlastigen und intensiv genutzten Enterprise-Anwendungen sowie Traffic-Optimierung abgestimmt.

Diese Lösungen eignen sich ideal für traditionelle wie virtualisierte Rechenzentren und Cloud-Infrastrukturen in Unternehmen aller Größenordnungen.

■ Fortinet AscenLink

WAN Link Load Balancing

Fortinet-AscenLink-Lösungen ermöglichen intelligentes Load Balancing sowohl des Internet als auch des Intranet Verkehrs über viele WAN-Verbindungen hinweg. Auf diese Weise wird kostengünstig Bandbreite für ein und ausgehende Verbindungen bereitgestellt sowie die Zuverlässigkeit der Verbindungen erhöht. Die Benutzeroberfläche ist sehr anwenderfreundlich und bietet ein flexibles Regel-basierendes Performancemanagementsystem.

Die wesentlichen Merkmale dieser Lösungen sind:

- Steigerung der Netzwerkleistung durch intelligente Verteilung der Last auf alle verfügbaren WAN-Leitungen
- kostengünstige Site-to-Site WAN-Verbindungen durch Nutzung vieler kostengünstiger Internetzugänge anstelle weniger teurer Anschlüsse
- Load Balancing von Service Anfragen von Internetanwendern auf Web, E-Mail oder VPN-Server
- 7 verschiedene Load Balancing Algorithmen

■ FortiCache

Bandbreite – eine ständige Herausforderung

Durch die Verlagerung der Internet-Nutzung von stationären zu mobilen Endgeräten haben sich die Nutzungsprofile ebenso drastisch verändert wie die Art und Menge der übertragenen Daten: Interaktive Webseiten, Video- und Audio-Streams und ständig größere Grafik-Dateien und Präsentationen erzeugen eine immense Last. Carrier, Service Provider, Großunternehmen und Schulungsanbieter kämpfen gemeinsam mit demselben Problem: Bandbreite ist bereits in dem Moment verbraucht, in dem sie bereitgestellt wird. Netzwerke müssen die explosionsartig steigende Nachfrage ebenso verkraften wie Engpässe verhindern und die Funktionalität und Profitabilität aufrecht erhalten werden müssen.

Kontrolle über das Netzwerk

Die FortiCache Appliances ermöglichen eine verbesserte Netzwerk-Kontrolle durch die Möglichkeit, Inhalte zu cachen (zwischenzuspeichern) und Anwendungen massiv zu beschleunigen – und reduzieren so deren Einfluss auf die Netzwerk-Performance. Durch das Cachen von Anwendungs-Inhalten können Großunternehmen ISPs, Mobilfunk-Provider, Telcos, Universitäten und andere Ausbildungs- Netzwerke häufig genutzte Daten einfach lokal bereitstellen und den mehrfachen Download verhindern.

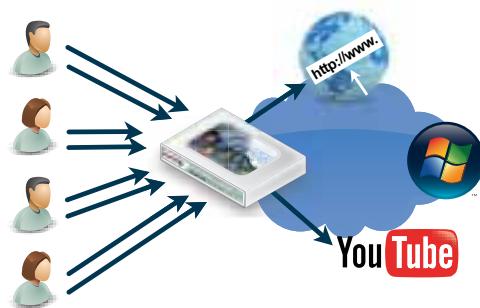
Bandbreiten-Reduktion und Applikations-Beschleunigung

Kurzzeitphänomene wie aktuelle Nachrichten, Sport-Events, Videos, Spiele uvm. treiben Bandbreite-Anforderungen kurzzeitig in ultimative Höhen – um ebenso schnell wieder zu verschwinden. Durch diese unvorhersehbare, aber extrem hohe Nachfrage können ganze Netzwerke vorübergehend zusammenbrechen und wichtige Dienste nicht mehr verfügbar sein – was nicht selten hohe Kosten verursacht. Diese Spitzenlasten zu bewältigen, ermöglicht es den zuvor genannten Unternehmen, deutlich verbesserte Services bereitzustellen und damit Kunden- und Mitarbeiterzufriedenheit, Produktivität und letztlich Profitabilität spürbar zu steigern.

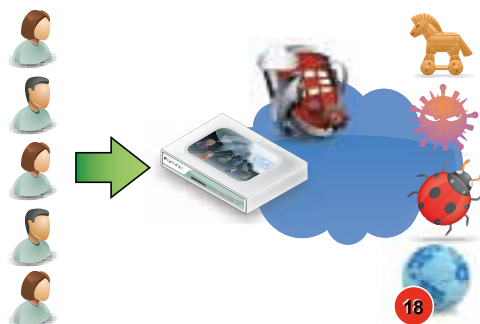
FortiCache Netzwerkkontrolle

Nicht überall ist Bandbreite zu vertretbaren Kosten oder unbegrenzt verfügbar. Oft sind hier kostspielige Alternativen wie etwa Satellitenverbindungen o. ä.

erforderlich, um die geforderten Dienste bereitstellen zu können. FortiCache behebt dieses Problem durch maximale Speicherung von Daten „im Netz“ und reduziert so spürbar die benötigte Leitungskapazität und damit die Kosten. FortiCache „versteht“ die Dateiformate von Content Delivery Networks (CDNs) wie z. B. YouTube und anderen Media-Streams, auch wenn diese Dateien mit Werbung versehen sind oder über verteilte Lokationen bereitgestellt werden.



Content-Caching



AntiVirus und URL-Filter



WAN-Optimierung

■ FortinetVM

Fortinet-Lösungen auch für VM-Systeme

Security Lösungen für virtualisierte Umgebungen – sog. Virtual Appliances – erlauben nun auch die Integration der bekannten und umfangreichen Fortinet-Security Lösungen in kritische, virtualisierte Infrastrukturen. Darüber hinaus ermöglichen Sie die kurzfristige Bereitstellung von Security-Diensten wann und wo auch immer sie benötigt werden.

Da Unternehmen inzwischen selten eine reine hardware-basierte oder reine virtuelle Infrastruktur betreiben, ist es sinnvoll, bedarfsabhängig beide Lösungen zu integrieren. In Kombination mit den höchst leistungsfähigen Fortinet-Appliances können Unternehmen somit einen Mix aus Soft- und Hardware-basierter Security Infrastruktur implementieren. Fortinet bietet bereits seit 2004 virtualisierte Security-Lösungen an, die heute von vielen Service-Providern und Großkonzernen genutzt werden, um flexibel und mandantenfähig komplexe Sicherheits-Dienste anbieten zu können.

Mit der FortinetVM Serie erweitert Fortinet dieses Angebot für VMware und XEN Plattformen und ermöglicht noch weiterreichende Flexibilität. So können Unternehmen eine verteilte Infrastruktur sowohl hardware-basiert als auch virtualisiert nutzen und zentral mit nur einer Management-Instanz administrieren. Auch FortiManager und FortiAnalyzer sind als virtualisierte Lösungen verfügbar und integrieren sich so in ein schlüssiges Konzept.

Lösungen für MSSPs

Durch ein speziell beim FortiAnalyzer adaptiertes neues und additives Lizenzmodell können nun individuelle Security-Services seitens eines Managed Security Service Providers einfach und mit planbaren Kosten bereitgestellt werden. So kann die gesamte Infrastruktur – oder Teile derselben – auf virtuellen Systemen abgebildet werden. Bereits vorhandene Plattformen können so optimal genutzt und die benötigten Services bedarfsgerecht skaliert werden.

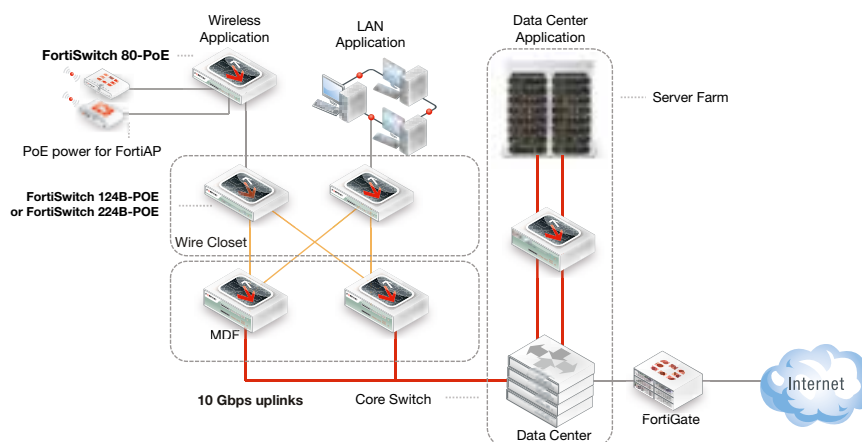
ZUBEHÖR

■ FortiSwitch

Gigabit Ethernet Switches

Fortinets FortiSwitch Gigabit Ethernet Switch Familie mit 10 Gigabit Ethernet Uplinks bietet hohe Performance und Skalierbarkeit zu einem günstigen Preis. Die FortiSwitch Plattform ist für High-Performance Computing (HPC) entwickelt worden und bietet dabei

Einsatzmöglichkeiten für jede Umgebung – von Small Office bis hin zum Data Center. Die den FortiSwitches zugrundeliegende Technologie wurde zudem auch in alle HighEnd FortiGate Systeme integriert.



■ Network Access Control

Mit den neueren FortiGate und FortiSwitchOS-Releases (ab 5.2.) ist das zentrale NAC-Management der Switch-Ports auch über eine FortiGate möglich. Somit kann Sicherheit zentral administriert werden, ohne auf

Flexibilität und Performance zu verzichten. Gleichzeitig werden Kosten gesenkt und Bedienerfreundlichkeit ein weiteres Mal erhöht.

■ PoE-Support

Viele der Switches verfügen – ähnlich wie einige FortiGate Modelle – über Power over Ethernet (PoE) Support. Damit ist es einfach möglich, über das Netzwerkkabel die angeschlossenen Endgeräte

wie AccessPoints, IP-Kameras oder IP-Telefone, mit der benötigten Betriebsspannung zu versorgen. Eine zusätzliche Stromversorgung kann so entfallen.



■ FortiCam und FortiRecorder

IP-basierte Gebäudeüberwachung

Mit FortiCamera lösen Sie ihre Probleme bei der Videoüberwachung und verbessern das Nutzererlebnis. Sichern Sie Ihre Eingänge und kritischen Bereiche, wie Verkaufsterminals, Lagerhäuser, öffentliche Bereiche und Laderampen mit Kameras ab. Die Bilder werden vom Netzwerk-VideoRecorder aufgezeichnet. Die Videoüberwachung wird somit zu einer Erweiterung Ihres Netzwerks.



■ Appliance oder VM ohne Lizenzgebühren

FortiCameras erfordern keinerlei Softwareinstallation, Patches oder nutzerbasierte Lizenzgebühren. FortiCamera ist einfach. Verbinden Sie die Kamera, schalten Sie die Appliance an, öffnen Sie einen Webbrowser, und alles ist einsatzbereit. Der FortiRecorder ist ebenfalls als virtuelle Maschine erhältlich.



■ FortiBridge

Hardware-FailOver-System

FailOver-Schutz für FortiGate Appliances, die online genutzt werden. Überbrückt die Verbindung ohne Unterbrechung bei System- oder Stromausfall.

■ PoE Power-Injector

Der PoE-Power-Injector ermöglicht die Spannungsversorgung von PoE-fähigen Endgeräten wie den FortiAP-WLAN-Access-Points oder FortiFon-VoIP-Telefonen auch an FortiGate Appliances oder Switches ohne PoE-Support.

■ Rackmount Kits

Fortinet bietet hochleistungsfähige Geräte für kleine und mittlere Unternehmen – allerdings handelt es sich dabei um Desktop-Modelle. Derzeit steigen immer mehr Unternehmen auf 19-Zoll-Racks um. Die neuen FortiRack-Kits eignen sich dabei hervorragend für den Einbau von Fortinet-Geräten in 19-Zoll-Schaltschränke. Das FortiRack-Kit ist die ideale Ergänzung, für den Einbau der hochleistungsfähigen FortiGate Einheit in einem 19-Zoll-Rack. Darüber hinaus werden so die wichtigsten Konsolen- und Netzwerkverbindungen an die Vorderseite verlagert. Der Zusammenbau ist in nur fünf Minuten erledigt. Hierzu wird einfach die FortiGate Einheit in den Kit eingesetzt, die Halter angebracht und die mitgelieferten Kabel werden mit den Keystones verbunden. FortiRacks gibt es für alle Geräte der Baureihen FortiGate, FortiAnalyzer, FortiManager & FortiMail, die nicht in ein Rack passen.

Dienste

■ FortiCare™

Unsere Kundensupportorganisation FortiCare bietet weltweiten TechniksUPPORT für alle Fortinet Produkte mit Supportmitarbeitern in Amerika, Europa, dem Nahen Osten und Asien. FortiCare-Support bietet Dienstleistungen für Unternehmen jeder Größe.

- **Erweiterter 8x5-Support** – Für Kunden, die Support während der örtlichen Geschäftszeiten benötigen.
- **Umfassender 24x7-Support** – Für Kunden, die rund um die Uhr wichtigen Support benötigen, einschließlich erweitertem Hardware-Austausch.
- **Premiumdienste** – Für Kunden, die einen zuständigen Technischen Kundenbetreuer, spezielle

Servicevereinbarungen, erweiterten Softwaresupport, priorisierte Steigerung bei dringenden Angelegenheiten, regelmäßige Konferenzen, Besuche und mehr benötigen. Es sind sowohl regionale als auch globale Pakete erhältlich.

- **Professionelle Dienste** – Für Kunden mit komplexeren Sicherheitssystemen, die konzentrierte Planung, umfassende Tests, effektiven Wissenstransfer und nahtlose Verwaltung benötigen. Zu den Professionellen Diensten gehören Architektur- und Designdienste, Umsetzungs- und Ausführungsdienste, Übergangsdienste und betriebliche Dienste. Für alle gibt es flexible Bereitstellungsmethoden.

■ FortiGuard™

Gefahrenforschung und Umgang

Das globale Forschungsteam unseres FortiGuard Lab untersucht ständig die Entwicklung neuer Gefahren. Über 200 Forscher stehen rund um die Uhr zur Verfügung, damit Ihr Netzwerk bestens geschützt ist. Sie liefern schnelle Produkt-Updates und detaillierte Kenntnisse, um Sie vor den neusten Gefahren zu schützen.

Training und Zertifizierung

Werden Sie Fortinet Netzwerksicherheitsexperte! Der Fortinet Network Security Expert (NSE) ist ein neues, achtstufiges Zertifizierungsprogramm für Techniker, die an einer unabhängigen Zertifizierung ihrer Netzwerksicherheitsfähigkeiten und ihrer Erfahrung interessiert

sind. Das Programm umfasst eine große Auswahl an autodidaktischen und geführten Kursen sowie praktische experimentelle Aufgaben, die die Beherrschung komplexer Netzwerksicherheitskonzepte demonstrieren. NSE wurde für Kunden, Partner und Mitarbeiter entwickelt und ermöglicht den Teilnehmern, das volle Potential der Netzwerksicherheitsplattform von Fortinet auszuschöpfen und als Angehöriger einer erlesenen Gruppe von Sicherheitsprofis anerkannt zu werden.

Mehr Informationen finden Sie auf
www.fortinet.com/training/nse.html

FortiGate® Network Security Platform - *Top Selling Models Matrix

	FG/FWF-30D	FG/FWF-60D	FG-80D	FG-70D, FG/FWF-90D	FG/FWF-92D	FG-100D	FG-200D	FG-300D	FG-500D	FG-800C
Firewall Throughput (1518/512/64 byte UDP)	0.8 / 0.8 / 0.8 Gbps	1.5 / 1.5 / 1.5 Gbps	1.3 / 0.95 / 0.17 Gbps	3.5 / 3.5 / 3.5 Gbps	2.0 / 1.0 / 0.2 Gbps	2.5 / 1 / 0.2 Gbps	3 / 3 / 3 Gbps	8 / 8 / 8 Gbps	16 / 16 / 16 Gbps	20 / 20 / 20 Gbps
Firewall Latency	8 µs	4 µs	90 µs	4 µs	46 µs	37 µs	2 µs	3 µs	3 µs	6 µs
Concurrent Sessions	200,000	500,000	1.5 Million	2 Million	1.5 Million	3 Million	3.2 Million	6 Million	6 Million	7 Million
New Sessions/Sec	3,500	4,000	22,000	4,000	22,000	22,000	77,000	200,000	280,000	190,000
Firewall Policies	5,000	5,000	5,000	5,000	5,000	10,000	10,000	10,000	10,000	10,000
IPSec VPN Throughput	350 Mbps	1 Gbps	200 Mbps	1 Gbps	130 Mbps	450 Mbps	1.3 Gbps	7 Gbps	14 Gbps	8 Gbps
Max G/W to G/W IPSEC Tunnels	20	200	200	200	200	2,000	2,000	2,000	2,000	2,000
Max Client to G/W IPSEC Tunnels	250	500	1,000	1,000	1,000	5,000	5,000	10,000	10,000	50,000
SSL VPN Throughput	25 Mbps	30 Mbps	130 Mbps	35 Mbps	170 Mbps	300 Mbps	400 Mbps	350 Mbps	400 Mbps	1.3 Gbps
Recommended SSL VPN Users	80	100	200	200	200	300	300	500	500	10,000
IPS Throughput	150 Mbps	200 Mbps	800 Mbps	275 Mbps	950 Mbps	950 Mbps	1.7 Gbps	2.8 Gbps	4.7 Gbps	6 Gbps
Antivirus Throughput (Proxy-Based/ Flow-Based)	30 / 40 Mbps	35 / 50 Mbps	250 / 550 Mbps	35 / 65 Mbps	300 / 700 Mbps	300 / 700 Mbps	600 / 1,100 Mbps	1.4 / 2.5 Gbps	1.7 / 3.4 Gbps	1.7 / 3.1 Gbps
Max FortiAPs (Total / Tunnel)	2 / 2	10 / 5	32 / 16	32 / 16	32 / 16	64 / 32	128 / 64	512 / 256	512 / 256	1024 / 512
Max FortiTokens	20	100	100	100	100	1,000	1,000	1,000	1,000	1,000
Max Registered FortiClient	200	200	200	200	200	600	600	600	2,000	2,000
Virtual Domains (Default/Max)	-	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10
Interfaces	5x GE RJ45	10x GE RJ45	4x GE RJ45	16x GE RJ45	16x GE RJ45	20x GE RJ45, 2x Shared Port Pairs (100D only)	18x GE RJ45, 2x GE SFP	6x GE RJ45, 4x GE SFP	10x GE RJ45, 8x GE SFP	2x 10GE SFP+, 14x GE RJ45, 8x Shared Port Pairs, 2x Bypass Pairs
Local Storage	-	-	16 GB	FG/FWF-90D: 32 GB	16 GB	32 GB	64 GB	120 GB	120 GB	60 GB
Power Supplies	Single AC Power Supply	Single AC Power Supply	Single AC Power Supply	Single AC Power Supply	Single AC Power Supply	Single AC Power Supply	Single AC Power Supply, opt. Ext RPS	Single AC Power Supply, opt. Ext RPS	Single AC Power Supply, opt. Ext RPS	Single AC Power Supply, opt. Dual PS or Ext RPS
Form Factor	Desktop	Desktop	Desktop	Desktop	Desktop	Rack Mount, 1 RU	Rack Mount, 1 RU	Rack Mount, 1 RU	Rack Mount, 1 RU	Rack Mount, 1 RU
Variants	WiFi, POE	WiFi, POE, LENC	-	WiFi, POE, LENC, High port density + POE	WiFi	LENC, High port density, High port density + POE	LENC, POE, High port density, High port density + POE	-	-	DC

	FG-1000D	FG-1200D	FG-1500D	FG-3240C	FG-3200D	FG-3700D	FG-3810D	FG-3950B	FG-5001C	FG-5001D
Firewall Throughput (1518/512/64 byte UDP)	52 / 52 / 33 Gbps	72 / 72 / 50 Gbps	80 / 80 / 55 Gbps	40 / 40 / 40 Gbps	80 / 80 / 50 Gbps	160 / 160 / 110 Gbps	320 / 320 / 175 Gbps	20-120 / 20-120 / 20-120 Gbps	40 / 40 / 40 Gbps	80 / 80 / 45 Gbps
Firewall Latency	3 µs	3 µs	3 µs	4 µs	3 µs	2 µs	5 µs	4 µs	4 µs	3 µs
Concurrent Sessions	11 Million	11 Million	12 Million	10 Mil	50 Million	50 Million	95 Million	20 Million	29.5 Million	23 Million
New Sessions/Sec	240,000	240,000	250,000	200,000	280,000	400,000	480,000	250K - 300K**	210,000	565,000
Firewall Policies	100,000	100,000	100,000	100,000	100,000	100,000	100,000	100,000	100,000	100,000
IPSec VPN Throughput	30 Gbps	40 Gbps	50 Gbps	17 Gbps	50 Gbps	100 Gbps	135 Gbps	8 - 50.5 Gbps	17 Gbps	25 Gbps
Max G/W to G/W IPSEC Tunnels	20,000	20,000	20,000	20,000	20,000	40,000	40,000	40,000	40,000	40,000
Max Client to G/W IPSEC Tunnels	50,000	50,000	50,000	64,000	64,000	64,000	64,000	64,000	64,000	64,000
SSL VPN Throughput	3.6 Gbps	3.6 Gbps	4 Gbps	3.4 Gbps	8 Gbps	10 Gbps	10 Gbps	1.2 Gbps	3.6 Gbps	6.5 Gbps
Recommended SSL VPN Users	10,000	10,000	10,000	30,000	30,000	30,000	30,000	25,000	20,000	25,000
IPS Throughput	8 Gbps	11 Gbps	11 Gbps	8 Gbps	14 Gbps	23 Gbps	25 Gbps	5 - 20 Gbps	12 Gbps	18 Gbps
Antivirus Throughput (Proxy-Based/ Flow-Based)	3.5 / 5.5 Gbps	3.5 / 10 Gbps	4.3 / 13 Gbps	2.6 / 9 Gbps	5.7 / 16 Gbps	7.5 / 18 Gbps	7.5 Gbps	4 / 5 - 15 Gbps	3 / 4 Gbps	5.6 / 13 Gbps
Max FortiAPs (Total, Tunnel)	4,096 / 1,024	4,096 / 1,024	4,096 / 1,024	4096 / 1024	4096 / 1024	4,096 / 1,024	4,096 / 1,024	4,096 / 1,024	4,096 / 1,024	4,096 / 1,024
Max FortiTokens	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000
Max Registered Endpoints	8,000	8,000	8,000	20,000	20,000	20,000	20,000	20,000	20,000	20,000
Virtual Domains (Default/Max)	10 / 250	10 / 250	10 / 250	10 / 500	10 / 500	10 / 500	10 / 500	10 / 500	10 / 500	10 / 500
Interfaces	2x 10 GE SFP+, 16x GE SFP, 18x GE RJ45	4x 10GE SFP+/GE SFP, 16x GE SFP, 18x GE RJ45	8x 10GE SFP+/GE SFP, 16x GE SFP, 18x GE RJ45	12x 10GE SFP+/GE SFP, 2x GE RJ45, 16x GE SFP	48x 10GE SFP+/GE SFP, 2x GE RJ45	4x 40GE QSFP+, 20x 10GE SFP+/GE SFP, 8x SFP+, 2x GE RJ45	6x 100GE CFP2, 2x GE RJ45	2x 10GE SFP+, 4x GE SFP, 2x GE RJ45	2x 10GE SFP+, 2x GE RJ45	2x 40GE QSFP+, 2x 10GE SFP+, 2x GE RJ45
Local Storage	120 GB	120 GB	240 GB	64 GB	960 GB	960 GB	960 GB	256 GB	128 GB	200 GB
Power Supplies	Dual PS	Dual PS	Dual PS	Dual PS	Dual PS	Dual PS	Dual PS	Dual PS	Chassis Based	Chassis Based
Form Factor	Rack Mount, 2 RU	Rack Mount, 2 RU	Rack Mount, 2 RU	Rack Mount, 2 RU	Rack Mount, 2 RU	Rack Mount, 3 RU	Rack Mount, 3 RU	Rack Mount, 3 RU	ATCA Blade	ATCA Blade
Variants	-	-	-	DC	-	DC	-	DC, LENC	-	-

* Featured Top selling models, for complete FortiGate offerings please visit www.fortinet.com. FortiGate virtual appliances are also available. Specifications based on FortiOS V5.2+
 ** With FMC-XHO

FortiManager™ Centralized Management Platform

	FMG-200D	FMG-300D	FMG-1000D	FMG-3900E	FMG-4000E	FMG-VM-BASE	FMG-VM-10-UG	FMG-VM-100-UG	FMG-VM-1000-UG	FMG-VM-5000-UG	FMG-VM-U-UG
Max Licensed Devices/ADoms	30	300	1,000	10,000	4,000	10	+10	+100	+1,000	+5,000	Unlimited
Max Web Portals/Users	-	-	1,000	10,000	4,000	10	+10	+100	+1,000	+5,000	Unlimited
GB Logs/Day	2	2	2	10	10	1	2	5	10	25	50
Locally Hosted Security Content	AV, IPS, VM, WF, AS	AV, IPS, VM, WF, AS	AV, IPS, VM, WF, AS	AV, IPS, VM, WF, AS	AV, IPS, VM, WF, AS	AV, IPS, VM	AV, IPS, VM	AV, IPS, VM WF, AS	AV, IPS, VM, WF, AS	AV, IPS, VM, WF, AS	AV, IPS, VM, WF, AS
Total Interfaces	4x GE RJ45	4x GE RJ45	6x GE RJ45, 2x SFP	2x GE, 2x GE SFP+	4x GE RJ45, 2x SFP	1 / 4 (vNIC Min / Max)					
Storage Capacity	1x 1 TB	2x 2TB	4x 2 TB	15x 960 GB	8x 2 TB	80 GB / 16 TB (Min / Max)					

FortiAnalyzer™ Centralized Logging & Reporting Solution

	FAZ-200D	FAZ-300D	FAZ-1000D	FAZ-2000B	FAZ-3000E	FAZ-3500E	FAZ-3900E	FAZ-VM-BASE	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100
GB Logs/Day	5	15	25	75	800	Unrestricted*	Unrestricted*	1	+1	+5	+25	+100
Sessions/Day	18 Mil	55 Mil	85 Mil	260 Mil	850 Mil	Unrestricted*	Unrestricted*	3.5 Mil	3.5 Mil	18 Mil	85 Mil	360 Mil
Peak Log Rate (standalone Mode)	350	625	1,000	5,000	50,000	60,000	75,000	-	-	-	-	-
Max. Licensed Devices/VDOMs/ADOMs	150	175	2,000	2,000	4,000	4,000	4,000	10,000	10,000	10,000	10,000	10,000
Total Interfaces	4x GE RJ45	4x GE RJ45	6x GE RJ45, 2x SFP	6x GE RJ45	4x GE RJ45, 2x GE SFP	2x GE RJ45, 2x GE SFP	2x GE RJ45, 2x GE SFP+	-	-	-	-	-
Storage Capacity	1x 1 TB	2x 2 TB	4x 2 TB	2x 2 TB (12 TB Max)	8x 2 TB (16 TB Max)	12x 2 TB (48 TB Max)	15x 960 GB	200 GB**	200 GB**	1 TB**	8 TB**	16 TB**
RAID Support	No	Yes (Mirrored)	Yes, (RAID 0, 1, 5, 6, 10, 50, 60)	0, 1, 5, 10, 50)	Yes, (RAID 0, 1, 5, 6, 10, 50, 60)	Yes, (RAID 0, 1, 5, 6, 10, 50, 60)	Yes, (RAID 0, 1, 5, 6, 10, 50, 60)	-	-	-	-	-

FortiAP™ (Indoor) Wireless Access Point

	FAP-24D	FAP-221B/223B	FAP-221C/223C	FAP-320B	FAP-320C	FAP-321C
Suggested Use Case	Low density indoor	Medium density indoor	Medium density indoor	Indoor high performance AP	high density 802.11ac, streaming app resilience	Medium density 802.11ac without resilience
IEEE Standard	802.11 a/b/g/n	802.11 a/b/g/n	802.11 a/b/g/n/ac	802.11 a/b/g/n	802.11 a/b/g/n/ac	802.11 a/b/g/n/ac
Number of Radio / Antennas	1 / 2 Internal	221B: 2 / 4 Int. 223B: 2 / 4 Ext.	221C: 2 / 4 Int. 223C: 2 / 4 Ext.	2 / 6 internal	2 / 6 internal	2 / 6 internal
MIMO (Total Association Rate)	2x2 MIMO dual spatial stream (300 Mbps Total)	2x2 MIMO dual spatial stream (600 Mbps Total)	2x2 MIMO dual spatial stream (1,167 Mbps Total)	3x3 MIMO with 3 spatial streams (900 Mbps Total)	3x3 MIMO with 3 spatial streams (1,750 Mbps Total)	3x3 MIMO with 3 spatial streams (1,750 Mbps Total)
Total (Client access + Monitoring) Simultaneous SSIDs	16	16	16	16	16	16
Max Transmission Power	18dBm (63mW)	17dBm (50mW)	20 dBm (100mW)	24 dBm (250mW) *	21 dBm (126mW) *	20 dBm (100mW)
Ethernet Interface	1x GE WAN, 4x FE LAN	1x GE RJ45	1x GE RJ45	2x GE RJ45	2x GE RJ45	1x GE RJ45
Power over Ethernet (PoE)	802.3af	802.3af	802.3af	802.3af	802.3af	802.3af

FortiSwitch™ Secured Access Switch

	FSW-28C	FSW-108D-POE	FSW-124D	FSW-124D-POE	FSW-224D-POE	FSW-324B-POE	FSW-348B	FSW-448B
Total Interfaces	8 x GE RJ45 LAN, 2 x GE RJ45 WAN	8x GE POE RJ45 ports, 2x Shared Port Pairs	24x GE RJ45, 2x GE SFP	24x GE RJ45 (incl. 12 PoE), 2x GE SFP	20x GE RJ45 (incl. 12 PoE), 4x GE Shared Port Pairs	16x GE PoE, 4x GE PoE+, 4x Shared Port Pairs	48 GE RJ45, 2x Shared Port Pairs	48 GE RJ45, 2x 10GE SFP+
Switch Capability	16 Gbps	20 Gbps	52 Gbps	52 Gbps	48 Gbps	48 Gbps	96 Gbps	136 Gbps
FortiGate Switch Controller Support	Yes (Remote)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

FortiAuthenticator™ User Identity Management Server

	FAC-200D	FAC-400C	FAC-1000D	FAC-3000D	FAC-VM Base	FAC-VM-100-UG	FAC-VM-1000-UG	FAC-VM-10000-UG	FAC-VM-100000-UG
Max Local/Remote Users/ User Group	500 / 500 / 25	2,000 / 2,000 / 50	10,000 / 10,000 / 2,000	40,000 / 40,000 / 4,000	100 / 100 / 10	+100 / +100 / +10	+1,000 / +1,000 / +100	+10,000 / +10,000 / +1,000	+100,000 / +100,000 / +10,000
Max FortiToken	500	2,000	10,000	40,000	200	+200	+2,000	+20,000	+200,000
Max NAS Devices	50	200	1,000	4,000	10	+10	+100	+1,000	+10,000

FortiSandbox™ Advanced Threat Prevention System

	FSA-1000D	FSA-3000D	FSA-VM
VM Sandboxing (Files/Hour)	160	560	Hardware dependent
AV Scanning (Files/Hour)	6,000	15,000	Hardware dependent
Number of VMs	8	28	4, up to 52

FortiDDOS™ Hardware Accelerated DDoS Mitigator

	FDD-200B	FDD-400B	FDD-800B	FDD-1000B	FDD-2000B
Throughput (Full Duplex)	2 Gbps	4 Gbps	8 Gbps	12 Gbps	24 Gbps
Simultaneous Connections	1 Mil	1 Mil	2 Mil	3 Mil	4 Mil
Session Setup/Teardown	100 K/Sec	100 K/Sec	200 K/Sec	300 K/Sec	600 K/Sec

FortiMail™ Messaging Security Server

	FML-200D	FML-400C	FML-1000D	FML-3000D	FML-VM00	FML-VM01	FML-VM02	FML-VM04	FML-VM08
Email Routing* (Msg/Hr)	76,000	150,000	680,000	1.5 Mil	3,600	34,000	67,000	306,000	675,000
Performance AS+AV* (Msg/Hr)	58,000	120,000	500,000	1.3 Mil	2,700	26,000	52,000	225,000	585,000
Email Domains	20	100	800	2,000	2	20	100	800	2,000
Server Mode Mailboxes	150	400	1,500	3,000	50	150	400	1,500	3,000
Storage Capacity	1x 1 TB	2x 1 TB	2x 2 TB	2x 2 TB (12 TB Max)	1x 146GB	50 GB - 1 TB	50 GB - 2 TB	50 GB - 4 TB	50 GB - 8 TB

FortiWeb™ Web Application Firewall

	FWB-400C	FWB-1000D	FWB-3000D/Fsx	FWB-4000D	FWB-VM01/-VM02/- VM04/-VM08
Throughput (HTTP)	100 Mbps	750 Mbps	1.5 Gbps	4 Gbps	25 Mbps /100 Mbps/ 500 Mbps 1 Gbps
Total Interfaces	4x GE RJ45	2x GE RJ45, 4x GE RJ45 Bypass, 2x GE SFP	6x GE RJ45, 2x GE Bypass /Fsx: 6x GE RJ45 , 2x 10GE SFP+ Bypass	6x GE RJ45, 2x GE RJ45 Bypass, 2x GE SX Bypass, 2x 10GE SFP+ Bypass	-

FortiADC™ Application Delivery Controller

	FAD-100E	FAD-200D	FAD-200E	FAD-300E	FAD-400E	FAD-600E	FAD-700D	FAD- 1000E	FAD- 1500D	FAD- 2000D	FAD- 4000D
Throughput (HTTP)	1 Gbps	2.7 Gbps	2.7 Gbps	4.8 Gbps	8 Gbps	12 Gbps	15 Gbps	15 Gbps	20 Gbps	30 Gbps	50 Gbps
Total Interfaces	4x GE RJ45	4x GE RJ45	4x GE RJ45	6x GE RJ45	8x GE RJ45	2x 10GE, 8x GE RJ45	4x 10 GE SFP+, 4x GE SFP, 4x GE RJ45	2x 10GE, 8x GE RJ45	4x 10GE, 8x GE RJ45	4x 10GE, 16x GE RJ45	8x 10GE, 16x GE RJ45

Virtual Appliance Support Matrix

	VMWare vSphere v4.0/4.1	VMWare vSphere v5.0/5.1/5.5	Citrix Xen Server v5.6 SP2	Citrix Xen Server v6.0	Xen	KVM	Amazon AWS	Microsoft Hyper-V 2008 R2	Microsoft Hyper-V 2012
FortiGate-VM	•	•	•	•	•	•	•*	•	•
FortiManager-VM	•	•					•	•	•
FortiAnalyzer-VM	•	•					•*	•	•
FortiWeb-VM	•	•		•	•		•		•
FortiMail-VM	•	•			•	•		•	•
FortiAuthenticator-VM	•	•						•	•
FortiADC-VM		•							
FortiCache-VM	•	•							
FortiVoice-VM		•		•		•			•
FortiRecorder-VM		•		•		•			•
FortiSandbox-VM		5.1/5.5							




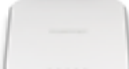
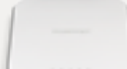
Also Available

[AscenLink](#) Link Load Balancer
[FortiBridge](#) Failopen Appliance
[FortiCache](#) Secure Web Cache
[FortiCamera](#) Network Video Security




[FortiClient](#) Host Security Client
[FortiDB](#) Database Security System
[FortiDirector](#) Cloud-based SLB System
[FortiDNS](#) Secure DNS Cache

[FortiExtender](#) 3G/4G WAN Extender
[FortiTap](#) Passive Network Tap
[FortiToken](#) 2 Factor Authentication Token
[FortiVoice](#) Secure VoIP Solution



FortiAP™ Indoor Thin Access Points

	FAP-210B	FAP-221B/223B	FAP-221C	FAP-320B	FAP-320C
					
Product Description	Indoor Access Point	Indoor Access Point / with external antennas	802.11ac Indoor Access Point	802.11n Enterprise Access Point	802.11ac Enterprise Access Point
Suggested Deployment	Indoor Motels, Clinics, Small Enterprise, Retail	Indoor Medium Enterprise, Hotels, Healthcare, Advanced Schools and Retail	Indoor Medium Enterprise, Hotels, Healthcare, Advanced Schools and Retail	Indoor Enterprises, Hotels, Healthcare, Advanced Schools, warehouse and Retail	Indoor Enterprises, Hotels, Healthcare, warehouse, Advanced Schools and Retail
Hardware					
Form Factor	Square	Round	Round	Square	Square
Dimension	1.1x6.4x5.1 in	6.5 x 1.2 in	6.5 x 1.5 in	6.5 x 6.5 x 1.6 in	6.5 x 6.5 x 1.4 in
Mounting	Wall; Ceiling with optional bracket	Drywall/T-Rail/Ceiling mounts included	Drywall/T-Rail/Ceiling mounts included	Drywall/T-Rail/Ceiling mounts included	Drywall/T-Rail/Ceiling mounts included
Kensington Lock	•	•	•	•	•
Ethernet Interfaces	1x GE RJ45	1x GE RJ45	1x GE RJ45	2x GE RJ45	2x GE RJ45
PoE	802.3af	802.3af	802.3af	802.3af	802.3af
Maximum power draw	12.9 W	12.9 W	12.9 W	12.9W	12.9W
Included accessories	AC adaptor, anchors	Mounting kits, anchors	Mounting kits, anchors	Mounting kits, anchors	Mounting kits, anchors
Resilient POE backup				•	•
Plenum installable				•	•
Mesh capable	•	•	•	•	•
Wireless					
IEEE Standard	802.11 a/b/g/n	802.11 a/b/g/n	802.11 a/b/g/n/ac	802.11 a/b/g/n	802.11 a/b/g/n/ac
Number of Radios	1	2	2	2	2
Radio Band	Dual	Dual	Dual	Dual	Dual
Radio 1 Band (association rate)	2.4 GHz / 5GHz (300 Mbps)	221B: 2.4 GHz / 5GHz, 223B: 5 GHz (300 Mbps)	2.4 GHz / 5GHz (300 Mbps)	2.4 GHz (450 Mbps)	2.4 GHz (450 Mbps)
Radio 2 Band (association rate)	-	2.4 GHz	5GHz (867 Mbps)	5 GHz (450 Mbps)	5 GHz (1300 Mbps)
MIMO	2x2 (dual stream)	2x2 (dual stream)	2x2 (dual stream)	3x3 (3 stream)	3x3 (3 stream)
Max / recommended number of concurrent clients	no limit / 30	no limit / 30 per radio	no limit / 30 per radio	no limit / 50 per radio	no limit / 50 per radio
Antenna Type and Count	2 - Internal	221B: 4 - Internal 223B: 4 - External	4 - Internal	6 - Internal	6 - Internal
Antenna Gain	3dBi/(4dBi-5GHz)	3dBi/(4dBi-5GHz)	3.5dBi/(6dBi-5GHz)	5dBi/(6dBi-5GHz)	5dBi/(6dBi-5GHz)
Max TX Power	17 dBm (50mW)	17 dBm (50mW)	20 dBm (100mW)	24 dBm (250mW)	21 dBm (126mW)
Number of SSIDs	8 (7 client, 1 monitor)	16 (14 client, 2 monitor)	16 (14 client, 2 monitor)	16 (14 client, 2 monitor)	16 (14 client, 2 monitor)
Traffic Queues	4 queues	4 queues	4 queues	4 queues	4 queues
802.11n 20/40MHz HT	•	•	•	•	•
802.11n MPDU/MSDU agg		•	•	•	•
802.11n Dynamic MIMO PS		•	•	•	•
802.11n LDPC encoding		•	•	•	•
802.11n MLD		•	•	•	•
802.11n Max ratio combining		•	•	•	•
802.11ac 80 MHz channel			•		•
Rogue AP scanning					
Dual Band Scanning	•	•	•	•	•
Background Scan	•	•		•	
Full-time dedicated monitor	•	•	•	•	•
Single Radio Dual band scanning		•	•		
On-wire MAC address collector	•	•	•	•	•
Management					
WebUI & CLI	•	•	•	•	•
External serial console port	•			•	•
Cloud deployment/management^	•	•	•	•	•
Controller discovery: DNS, DHCP, over L3 boundary	•	•	•	•	•
Certifications					
Wi-Fi Alliance Certified*		•	•	•	•
DFS Certified**		221B: Region E, J	Region E, J	Region E	Region E, A, J






FortiAP™ Remote Thin Access Points

	FAP-11C	FAP-14C	FAP-28C		
					
Product Description	Plug & Play Remote Access Point	Remote Access Point	Remote Access Point		
Suggested Deployment	SOHO, Travel, indoor	SOHO, Branch Office, Retail analytic sensor, indoor	SOHO, Branch Office, indoor		
Hardware					
Form Factor	Wall Plug	Desktop	Desktop		
Dimension	4.3 x 3.5 x 1.5 in / 110 x 89 x 34 mm	1.06 x 4.92 x 3.86 in / 27 x 125 x 98 mm	1.38 x 8.43 x 7.09 in / 35 x 214 x 180 mm		
Mounting	Wall Plug	Wall Mountable	Wall Mountable		
Kensington Lock			•		
Ethernet Interfaces	2x GE RJ45	5x FE RJ45	10x GE RJ45		
PoE					
Maximum power draw					
Included accessories	Power plugs	AC adaptor	AC adaptor		
Resilient POE backup					
Plenum installable					
Mesh capable	•	•	•		
Wireless					
IEEE Standard	802.11 b/g/n	802.11 b/g/n	802.11 a/b/g/n		
Number of Radios	1	1	1		
Radio Band	Single	Single	Single		
Radio 1 Band (association rate)	2.4 GHz (150 Mbps)	2.4 GHz (150 Mbps)	2.4 GHz / 5GHz (300 Mbps)		
Radio 2 Band (association rate)	-	-	-		
MIMO	1x1 (1 stream)	1x1 (1 stream)	2x2 (dual stream)		
Max / recommended number of concurrent clients	no limit / 5	no limit / 10	no limit / 20		
Antenna Type and Count	1 - Internal	1 - Internal	2 - Internal		
Antenna Gain	2dBi	2dBi	3dBi/(4dBi-5GHz)		
Max TX Power	17 dBm (50mW)	17 dBm (50mW)	17 dBm (50mW)		
Number of SSIDs	8 (7 client, 1 monitor)	8 (7 client, 1 monitor)	8 (7 client, 1 monitor)		
Traffic Queues	4 queues	4 queues	4 queues		
802.11n 20/40MHz HT					
802.11n MPDU/MSDU agg					
802.11n Dynamic MIMO PS					
802.11n LDPC encoding					
802.11n MLD					
802.11n Max ratio combining					
802.11ac 80 MHz channel					
Rogue AP scanning					
Dual Band Scanning					
Background Scan					
Full-time dedicated monitor					
Single Radio Dual band scanning					
On-wire MAC address collector					
Management					
WebUI & CLI	•	•	•		
External serial console port					
Cloud deployment/manage-ment^	•	•	•		
Controller discovery: DNS, DHCP, over L3 boundary	•	•	•		
Certifications					
Wi-Fi Alliance Certified*					
DFS Certified**					

FortiAP™ Outdoor/Indoor Thin Access Points

	FAP-112B	FAP-222B			
					
Product Description	Outdoor Access Point	Rugged Outdoor Access Point			
Suggested Deployment	Small Outdoor, indoor corridors	Outdoor deployments, warehouse			
Hardware					
Form Factor	IP55 enclosure	IP67 enclosure			
Dimension	7.3 x 2.6 x 1.3 in	2.75 x 7.75x10in			
Mounting	Wall/Pole, drywall anchors	Wall or Pole with kit included			
Kensington Lock					
Ethernet Interfaces	2x FE RJ45	1x GE RJ45			
PoE	Proprietary	802.3at & proprietary			
Maximum power draw	12.9 W	25 W			
Included accessories	AC adaptor & proprietary POE injector	AC adaptor & proprietary POE injector, outdoor Kit			
Resilient POE backup					
Plenum installable					
Mesh capable	•	•			
Wireless					
IEEE Standard	802.11 b/g/n	802.11 a/b/g/n			
Number of Radios	1	2			
Radio Band	Single	Dual			
Radio 1 Band (association rate)	2.4 GHz (150 Mbps)	2.4 GHz (300 Mbps)			
Radio 2 Band (association rate)	-	5 GHz (300 Mbps)			
MIMO	1x1 (1 stream)	2x2 (dual stream)			
Max / recommended number of concurrent clients	no limit / 30	no limit / 30 per radio			
Antenna Type and Count	1 - Internal	4 N-type External			
Antenna Gain	8dBi	5dBi/(7dBi-5GHz)			
Max TX Power	24 dBm (250mW)	27dBm (500mW)			
Number of SSIDs	8 (7 client, 1 monitor)	16 (14 client, 2 monitor)			
Traffic Queues	4 queues	4 queues			
802.11n 20/40Mhz HT		•			
802.11n MPDU/MSDU agg					
802.11n Dynamic MIMO PS					
802.11n LDPC encoding					
802.11n MLD	•				
802.11n Max ratio combining	•				
802.11ac 80 MHz channel					
Rogue AP scanning					
Dual Band Scanning		•			
Background Scan		•			
Full-time dedicated monitor		•			
Single Radio Dual band scanning					
On-wire MAC address collector	•	•			
Management					
WebUI & CLI	•	•			
External serial console port					
Cloud deployment/manage-ment^	•	•			
Controller discovery: DNS, DHCP, over L3 boundary	•	•			
Certifications					
Wi-Fi Alliance Certified*		•			
DFS Certified**					

FortiWiFi™ Indoor Thick Access Points

	FWF-30D	FWF-60D	FWF-80CM	FWF-90D	FWF-92D
					
Suggested Deployment	Home/small office	Distributed office	Distributed office	Indoor Motels, Clinics, Small Enterprise, Retail	Indoor Motels, Clinics, Small Enterprise, Retail
Hardware					
Form Factor	Desktop	Desktop	Desktop	Desktop	Desktop
Dimension	1.38 x 7.17 x 5.24 in	1.50 x 8.50 x 5.83 in	1.75 x 10.87 x 6.13 in	1.72 x 8.5 x 8.78 in	1.72 x 8.5 x 8.78 in
Mounting	Wall, desktop	Wall, desktop	Wall (optional kit with Lock), desktop	Wall, desktop	Wall, desktop
Kensington Lock	•		•	•	•
Ethernet Interfaces	1 x GE RJ45 WAN, 4 x GE RJ45 Switch ports	3 x GE RJ45 WAN/DMZ, 7 x GE RJ45 Switch ports	2 x GE RJ45 WAN, 1 x FE RJ45 DMZ, 6 x FE RJ45 Switch ports	2 x GE RJ45 WAN ports, 14 x GE RJ45 Switch ports	2 x GE RJ45 WAN ports, 14 x GE RJ45 Switch ports
Mesh Root		•	•	•	•
Other WiFi Variants	POE (PSE)	POE (PSE)	-	POE (PSE)	
Wireless					
IEEE Standard	802.11 a/b/g/n	802.11 a/b/g/n	802.11 a/b/g/n	802.11a/b/g/n	802.11a/b/g/n
Number of Radios	1	1	1	1	1
Radio Band	Dual	Dual	Dual	Dual	Dual
Radio 1 Band (association rate)	2.4GHz / 5GHz (300Mbps)	2.4GHz / 5GHz (300Mbps)	2.4GHz / 5GHz (300Mbps)	2.4GHz / 5GHz (300Mbps)	2.4GHz / 5GHz (300Mbps)
Radio 2 Band (association rate)	-	-	-	-	-
MIMO	2x2	2x2	2x3	2x2	2x2
Max / recommended number of concurrent clients	no limit / 30	no limit / 30	no limit / 30	no limit / 30	no limit / 30
Antenna Type and Count	2 F-type antennas	2 di-pole antennas	2 di-pole antennas	2 di-pole antennas	2 di-pole antennas
Antenna Gain	up to 5dB	up to 5dB	up to 5dB	up to 5dB	up to 5dB
Max TX Power	17dBm	17dBm	17dBm	17dBm	17dBm
Number of SSIDs	8 (7 client, 1 monitor)	8 (7 client, 1 monitor)	8 (7 client, 1 monitor)	8 (7 client, 1 monitor)	8 (7 client, 1 monitor)
Traffic Queues	4 queues	4 queues	4 queues	4 queues	4 queues
802.11n 20/40Mhz HT	•	•	•	•	•
Short Guard	•	•	•	•	•
802.11ac 80 MHz channel					
MAC Service Data Unit (MSDU) aggregation and MAC Protocol Data Unit (MPDU) frame aggregation	•	•	•	•	•
Cyclic-delay diversity (CDD)	•	•	•	•	•
Power Save (WME-PS)	•	•	•	•	•
802.11n Max ratio combining (MRC)	•	•	•	•	•
Transmit Beam Forming (TxBF)	•	•		•	•
Low Density Parity Check encoding (LDPC)	•	•		•	•
802.11n Maximum Likelihood Detection (MLD)	•	•	•	•	•
Rogue AP scanning					
Dual Band Scanning	•	•	•	•	•
Background Scan	•	•	•	•	•
Full-time dedicated monitor	•	•	•	•	•
Single Radio Dual band scanning	•	•	•	•	•
On-wire MAC address collector	•	•	•	•	•
Management					
WebUI & CLI	•	•	•	•	•
Max managed APs	2	10	32	32	32
Cloud deployment/manage-ment^	•	•	•	•	•
Certifications					
Wi-Fi Alliance Certified*					
DFS Certified**	Region: J	Region: J		Region: J	

FortiGate/FortiWiFi® Wireless Controller

	FortiGate/FortiWiFi 30D, 40C, 60C & 60D Series	FortiGate/FortiWiFi 80C & 90D Series	FortiGate 1xxC, 100D, 200B	FortiGate 200D Series	FortiGate 3xxB, 300C, 300D, 500D & 62xB
Hardware					
Product Range / Form Factor	Desktop / Desktop	Desktop / Desktop	Mid Range / 1 RU	Mid Range / 1-2 RU	Mid Range / 1 RU
GE Interfaces	5-10	2 - 16	8 - 40	18 - 88	10 - 18
GE PoE/PoE+ Interfaces	1-20 / 4 (FG-30D, 60D, 60C-POE)	4 (FG-90D-POE)	16 (FG-140D-POE)	8 (FG-200D-POE) 24 (FG-240D-POE) 32 (FG-280D-POE)	-
10 GE Interfaces	-	-	-	-	-
40 GE Interfaces	-	-	-	-	-
Capacity					
Maximum Supported APs (Tunnel Mode)	2 - 5	16	32	64	256
Maximum Supported APs (Total)	2 - 10	32	64	128	512
Max number of SSIDs	32	32	256	256	256
Max Concurrent Sessions	40 K - 1.5 Mil	1 - 1.5 Mil	1.4 - 3.2 Mil	1.4 Mil	2 Mil
	FortiGate 600C & 800C	FortiGate 1000 & 3000 Series	FG-5000 Series	FG-VM Series	
Hardware					
Product Range / Form Factor	Mid Range / 1 RU	High End / 2-3 RU	High End / 3-13 RU	-	
GE Interfaces	16-18	18 - 108	2 - 28	Refer to Datasheet	
GE PoE/PoE+ Interfaces	-	-	-	-	
10 GE Interfaces	0 - 2	2 - 28	2 - 112	Refer to Datasheet	
40 GE Interfaces	-	4	-		
Capacity					
Maximum Supported APs (Tun- nel Mode)	512	1,024	Up to 14,336 (1,024/blade)	32 - 1,024	
Maximum Supported APs (Total)	1,024	4,096	Up to 53,744 (4,096/blade)	64 - 4,096	
Max number of SSIDs	256	1,024	Up to 14,336 (1,024/blade)	32 - 1,024	
Max Concurrent Sessions	3 - 7 Mil	10 - 44 Mil	10 - 100 Mil	Refer to Datasheet	

* Certification covers following specifications: - 802.11a/b/g/n, Short Guard Interval, TX A-MPDU, STBC, 40 MHz operation in 5 GHz/WPA™ Personal, WPA™ Enterprise / Personal, WPA2™ , Enterprise / Personal, WMM™, EAP-TLS, EAP-TTLS/MSCHAPV2, PEAPv0/EAP-MSCHAPV2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST, 802.11 d/n, WMM Power Save.

** Requires latest FortiOS version.

^ Requires FortiOS V5.2.2+/FAP OS V5.2.2. Mass deployment is supported on all indicated models using FortiDeploy SKU. Single unit deployment only available if there's a sticker key attached to the item.

This document is provided as a convenient comparison of Fortinet products and services. The datasheet for any product or service can be found on www.fortinet.com should be consulted for the most updated specifications.

Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

FORTINET ÖSTERREICH

Wienerbergstraße 7/D, 1100 Wien

Tel: +43 1 22787 120

E-Mail: austria@fortinet.com

www.fortinet.com

FORTINET SCHWEIZ

Riedmuehlestrasse 8, Dietlikon 8305

Tel: +41 44 833 68 48

www.fortinet.com

